Engineering Change Notice

Hitachi Adaptable Modular Storage 2000 Series

ECN #	ECN DF800-512
Rev #	0
FCB #	n/a
Date	2014.08.29

Classification		S/W or F/W Changes		Application		S/W or F/W Code Type	
Hardware		New Features		Mandatory		Q-Code (GA)	x
Firmware	x	Improvements	x	Recommended	x	T-Code (Test)	
Software / Maintenance Tool		Bug-Fixes	x	Optional		I-Code (ICS)	
Documentation		n/a				n/a (H/W)	
(check all that apply)		*(check all that apply)*		*(check only one)*		*(check only one)*	

Title

Release of new Firmware <DF800 Ver. 08C3/U>

Purpose

This ECN is to inform of the release of new Firmware <DF800 Ver. 08C3/U (V12.3/U)>.

Description of Release

1. Supported features and functions

1.1 New function

None

1.2 Improvement

Please refer to Appendix-C.

1.3 Countermeasure

Please refer to Appendix-A.

2. Firmware Version List

The new Firmware for DF includes following versions.

No.	Program name			New Version	Previous Version Notified by ECN DF800-510
1	Firmware			08C3/U (*)	08C3/S (*)
2	Firmware	DF800	DF800S	08C3/U -S	08C3/S -S
3			DF800M	08C3/U -M	08C3/S -M
4			DF800H	08C3/U -H	08C3/S -H
5		DF800E	DF800ES	08C3/U -X	08C3/S -X
6			DF800EM	08C3/U -Y	08C3/S -Y
7			DF800EH	08C3/U -Z	08C3/S -Z
8	ENC Firmware	DF800/ DF800E	2.5 inch expansion unit	07-03-01	same as left
9			Other conventional units	06-10-06	same as left
10	HDD Firmware	AKF400(S)		4C0E	same as left
11		AKF400(S1)		5C07	same as left
12		AKH146(S)		4C63	same as left
13		AKH300(S)		4C63	same as left
14		AKH146(S1)		4C60	4C5D
15		AKH300(S1)		4C60	4C5D
16		AKH450(S)		4C60	4C5D
17		AKH300(S2)		5C5B	5C58
18		AKH450(S1)		5C5B	5C58
19		AKH450X(S1)		5C5B	5C58
20		AKH600(S)		5C5B	5C58
21		AKH600X(S)		5C5B	5C58
22		AKH146(H)		D06F	same as left
23		AKH146(H1)		D037	same as left
24		AKH300(H)		D037	same as left

25		AKH300(H1)	D017	same as left
26		AKH450(H)	D017	same as left
27		AKH146(H2)	D02L	same as left
28		AKH300(H2)	D02L	same as left
29		AKH450(H1)	D02L	same as left
30		AKH450X(H1)	D02L	same as left
31		AKH600(H)	D02L	same as left
32		AKH600X(H)	D02L	same as left
33		AMF300(H)	D028	same as left
34		AMF300(H)-J	D028	same as left
35		AMF600(H)	D028	same as left
36		AMF600(H)-J	D028	same as left
37		AMF300(H1)	H7H7	same as left
38		AMF600(H1)	H7H7	same as left
39	SSD Firmware	AKS200(T)	K008	same as left
40	SAS 7.2K	AWE2K(S)	5C05	same as left
41	Firmware	AWE2KX(S)	5C05	same as left
42	SED Firmware	ANH600(S)	5CE8	5CE5
43		ANH600X(S)	5CE8	5CE5

Note) Hatched indicates the changed items from the previous firmware release.
(*) Firmware for DF800, ENC Firmware, HDD Firmware, SSD Firmware, SAS 7.2K Firmware and SED Firmware are integrated into one packaged version to reduce handling complexity.

Related Program Versions

NO	Product Name	ECN No	New Version	Previous Version
1	Storage Navigator Modular2	ECN DFUTL-179	12.65	Same as left
2	Command Control Interface (RAID Manager)	ECN DF800-507	01-32-03/01	Same as left
3	RAID Manager LIB (RMLIB)	ECN DF800-421	01-16-03/01	Same as left
4	SNMP Agent Support Function MIB File	ECN DF800-470	21.0	Same as left
5	TDCONV4	ECN DF800-489	090A/A	Same as left

Related Document Versions

None

Related Part #s or Products

RKS/RKM/RKH/RKES/RKEM/RKEH

Field Change

None

Factory Shipment / Effective Date

None

Restrictions

None

Export Regulation

Refer to "The ECCN of the Program Product and Manual for DF Series" as follows.
For firmware (microcode): Program (DF800_SA800) sheet
For Maintenance Manual and User Guide: Manual (DF800_SA800) sheet

List of Appendices

Appendix	Appendix Title	File Name
A	Change of Contents	512Appendix_A.xls
C	DF800 Enhance/Countermeasure Items	512Appendix_C-DF800EnhanceItem.xls

ECN Revision History

Revision	Date	Written/Revised By	Description
0	2014.08.29	-	Original version.

Appendix-A Change of Contents

1	Title	Controller blockage at HDU link failure in RAID group without HDD redundancy
<1>	Phenomena	When an HDU link failure occurs in a RAID group that does not have HDD redundancy, a controller may be blocked. <Web Message> HG0312 Resource release time-out I30100 HDU error(Unit-yy,HDU-zz) yy:unit number, zz:HDU number
<2>	Severity	A: Critical High (Array System Outage /Data Disagreement) B: Critical Medium C: Critical Low
<3>	Conditions of Occurrence	The problem may occur when all of the following conditions are met. (1) 2 HDDs (3 HDDs in RAID6 configuration) are blocked in a RAID group. (2) In HDDs in use in the RAID group of (1), a link failure occurs frequently.
<4>	Probability of failure	Low <Explanation> The probability is low because whether the phenomenon becomes obvious or not depends on the timing when the check processing (several msec) of auto ENC firmware replacement in back-end diagnosis that runs at link failure and the periodical check processing (1-sec cycle) of auto ENC firmware replacement conflict each other.

<5>	Cause	Firmware bug When an HDD link failure occurs, the back-end diagnosis works and it performs the check processing of auto ENC firmware replacement. Meanwhile, the periodical check processing of auto ENC firmware replacement runs on one-second cycle. If the two check processings conflict, both processings wait for the completion of the other processing on each other and the both of them do not make progress, which eventually turns to time-out and the controller is blocked. <Countermeasure> The firmware is modified as follows. When the check processing of auto ENC firmware replacement by back-end diagnosis and the periodical check processing of auto ENC firmware replacement conflict each other, the former check processing runs first and then the latter runs.
<6>	Affected Products/Version	DF800S/M/H, V5.0/A (0850/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later
<7>	Fixed Product/Version	DF800S/M/H/ES/EM/EH, V12.3/U (08C3/U) and later
<8>	Recovery	Apply the fixed firmware. <Action in the case of the failure> Replace the blocked controller. <Web Message> HG0312 Resource release time-out I30100 HDU error(Unit-yy,HDU-zz) yy:unit number, zz:HDU number
	(1) Special direction (for the server settings/storages/other peripherals) to applying the modified code	None
	(2) Restriction of firmware exchange	None
	(3) others	None
<9>	Category	Backend
<10>	Changed Part	MICRO-Disk
<11>	Problem ID	VC3-0003 (Same as DF850 V77-0087)
<12>	Site	Customer
<13>	HDS Case No./ ESC/CTSC/APSC No.	HDS01161627 DF800-36553
<14>	Early Notice#	None

2	Title	DP optimization failed wrongly
<1>	Phenomena	When a user performs DP optimization, the DP optimization may turn to time-out and fail. <Web Message> I6HZ00 DP Pool Optimization failed(LU-X,Code-03) X:LU number
<2>	Severity	A: Critical High (Array System Outage /Data Disagreement) B: Critical Medium C: Critical Low
<3>	Conditions of Occurrence	The problem may occur when all the following conditions (1) to (4) are met if the firmware version is earlier than 08C1/A. The problem may occur when the following conditions (1) to (3) are met if the firmware version is 08C1/A or later. (1) Dynamic Provisioning is enabled. (2) Multiple DP RAID groups are created in a DP pool or multiple DP pools are created. (3) A user performs DP optimization for a DP volume in the DP pool. (4) After (3), the following operations or failures is performed or occurs. (4-1) The user deletes a DP pool different from that of (3). (4-2) An HDD constituting the DP pool is blocked. (4-3) In the DP RAID group that is in regression status before the operation (3), a failure occurs in an HDD in use. (4-4) A controller is blocked.
<4>	Probability of failure	Low <Explanation> The probability of failure is low because the problem becomes obvious when the following conditions is met in addition to those described in <3> Conditions of Occurrence. - A difference in the time kept inside controllers is 30 minutes or longer between two controllers.

<5>	Cause	Firmware bug The DP optimization processing de-stages the DP management information to an HDD and a core that has the ownership of alternative LU of primary pool monitors time-out. However, due to a bug that the DP optimization processing calculates the time required for de-staging wrongly if the core with the ownership of alternative LU of primary pool is switched by the condition (4) and there is 30-minute or longer difference in the time kept inside controller between two controllers, a time-out is detected for the de-staging and the DP optimization fails. <Countermeasure> The firmware is modified to correctly calculate the time required for de-staging of DP management information even when the core that has the ownership of alternative LU of primary pool is switched.
<6>	Affected Products/Version	DF800S/M/H, V8.0(0880/A) and later DF800ES/EM/EH, V9.0(0890/A) and later
<7>	Fixed Product/Version	DF800S/M/H/ES/EM/EH, V12.3/U (08C3/U) and later
<8>	Recovery	Apply the fixed firmware. <Action in the case of the failure> Perform the following operations. (1) Stop the DP optimization that ends abnormally. (2) Perform planned stop for the array system and then start it again. (3) Retry the DP optimization. <Web Message> I6HZ00 DP Pool Optimization failed(LU-X,Code-03) X:LU number
	(1) Special direction (for the server settings/storages/other peripherals) to applying the modified code	None
	(2) Restriction of firmware exchange	None
	(3) others	None
<9>	Category	Dynamic Provisioning
<10>	Changed Part	MICRO-Disk
<11>	Problem ID	VC4-0165
<12>	Site	Customer
<13>	HDS Case No./ ESC/CTSC/APSC No.	HDS01091411 DF800-57187
<14>	Early Notice#	None

3	Title	Wrongly reported message indicating "capacity of created DP volume exceeds alert threshold" at DP-VOL creation
<1>	Phenomena	When a DP-VOL is created, a Web message indicating "the capacity of created DP-VOL exceeds the alert threshold for over provisioning." may be reported wrongly. In this case, if [Yes] is specified for [Report] for [Over provisioning] and the E-Mail alert function and SNMP Agent Support function are used, mails and SNMP TRAP to report that "the capacity of created DP-VOL exceeds the alert threshold for over provisioning." are issued. <Web Message> I6GK00 Over Provisioning Ratio Forewarning(Pool-x) x:pool number
<2>	Severity	A: Critical High (Array System Outage /Data Disagreement) B: Critical Medium C: Critical Low
<3>	Conditions of Occurrence	The problem occurs when all of the following conditions are met. (1) Dynamic Provisioning is enabled. (2) The value of "the total DP pool capacity multiplied by the alert threshold for over provisioning" is greater than 137438953600. (When the alert threshold for over provisioning is 100% as default, if the total DP pool capacity is 1.28PB or greater, condition (2) is met.) (3) A user creates a DP-VOL.
<4>	Probability of failure	High <Explanation> The problem always occurs when the conditions of occurrence are met.

<5>	Cause	Firmware bug Whether the capacity of created DP-VOL exceed the capacity threshold or not is checked by calculating the capacity threshold from the total pool capacity and the alert threshold for over provisioning. However, the capacity threshold is smaller than what expected due to a bug in the calculation method for the capacity threshold. As a result, even when a DP-VOL whose capacity does not exceed the capacity threshold is created, the check processing wrongly determines that "the capacity of created DP-VOL exceeds the alert threshold" and reports related Web messages, mails, and SNMP TRAP. <Countermeasure> The firmware is modified to correctly calculate the capacity threshold from the total pool capacity and the alert threshold for over provisioning.
<6>	Affected Products/Version	DF800S/M/H, V7.0/A (0870/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later
<7>	Fixed Product/Version	DF800S/M/H/ES/EM/EH, V12.3/U (08C3/U) and later
<8>	Recovery	Apply the fixed firmware. <Action in the case of the failure> Change the value of alert threshold for over provisioning to be a smaller one so that the condition that the total DP pool capacity multiplied by the alert threshold for over provisioning is greater than 137438953600 is not met, or reduce the total DP pool capacity. <Web Message> I6GK00 Over Provisioning Ratio Forewarning(Pool-x) x:pool number
	(1) Special direction (for the server settings/storages/other peripherals) to applying the modified code	None
	(2) Restriction of firmware exchange	None
	(3) others	None
<9>	Category	Dynamic Provisioning
<10>	Changed Part	MICRO-Disk
<11>	Problem ID	VC4-0166 (Same as DF850 V77-0053)
<12>	Site	Domestic Customer
<13>	HDS Case No./ ESC/CTSC/APSC No.	None
<14>	Early Notice#	None

4	Title	Inadequate report of warning, "The DP volume capacity of the DP pool exceeded the Over Provisioning Ratio Forewarning threshold value"
<1>	Phenomena	If the difference in value between Warning Alert threshold and the Limit Alert threshold of Over Provisioning Threshold is less than 5%, a waning message; "The DP volume capacity of the DP pool exceeded the Over Provisioning Ratio Forewarning threshold value." is reported to users even though the DP pool capacity does not exceed the Warning Alert threshold. In this case, if [Yes] is specified for [Report] for [Over provisioning] and the E-Mail alert function and SNMP Agent Support function are used, mails and SNMP TRAP to report that "The DP volume capacity of the DP pool exceeded the Over Provisioning Ratio Forewarning threshold value." are issued. <Web Message> I6GK00 Over Provisioning Ratio Forewarning(Pool-x) x: pool number
<2>	Severity	A: Critical High (Array System Outage /Data Disagreement) B: Critical Medium C: Critical Low
<3>	Conditions of Occurrence	The problem occurs when all of the following conditions are met. (1) Dynamic Provisioning is enabled. (2) A DP pool is used. (3) The difference in value between Warning Alert threshold and the Limit Alert threshold of Over Provisioning Threshold for the DP pool of (2) is less than 5%. (Default: Limit Alert threshold is 130%, Warning Alert threshold is 100%.) (4) The total capacity of DP volumes created in the DP pool of (2) is 96% or more of the Limit Alert threshold, and is less than the Warning Alert threshold.
<4>	Probability of failure	High <Explanation> The problem always occurs when the conditions of occurrence are met.

<5>	Cause	Firmware bug When the occurrence conditions are met, the following expression is true. Capacity that is minus 5% of Limit Alert threshold < DP pool capacity< capacity of Warning Alert threshold Due to a bug that only "whether the DP pool capacity exceeds the capacity that is minus 5% of Limit Alert threshold" is checked, the firmware notifies users of the warning even though the DP pool capacity does not exceed the Warning Alert threshold. However, the notification of inadequate warning to users does not result in limitation on DP operations. <Countermeasure> The firmware is modified to check whether the DP pool capacity exceeds the Warning Alert threshold when the DP pool capacity exceeds the Limit Alert threshold, and notify users of warning if the DP pool capacity exceeds the Warning Alert threshold.
<6>	Affected Products/Version	DF800S/M/H, V7.0/A (0870/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later
<7>	Fixed Product/Version	DF800S/M/H/ES/EM/EH, V12.3/U (08C3/U) and later
<8>	Recovery	Apply the fixed firmware. <Action in the case of the failure> Change the Limit Alert threshold or Warning Alert threshold so that the difference between the thresholds is 5% or greater. <Web Message> Change the Limit Alert threshold or Warning Alert threshold so that the difference between the thresholds is 5% or greater.
	(1) Special direction (for the server settings/storages/other peripherals) to applying the modified code	None
	(2) Restriction of firmware exchange	None
	(3) others	None
<9>	Category	Dynamic Provisioning
<10>	Changed Part	MICRO-Disk
<11>	Problem ID	VC4-0167 (Same as DF850 V77-0082)
<12>	Site	Factory
<13>	HDS Case No./ ESC/CTSC/APSC No.	None

<14>	Early Notice#	None

Appendix C

DF800 Enhance/Countermeasure Items

Rev. 0

Class... N:NewFunction/Enhancement, I:Improvement, C:Countermeasure of problem at customer's cite
Level... A:Most important countermeasure for problem, B:Countermeasure for "medium" level issue, C:Countermeasure for "minor level " issue
For Example, A:System down, User Data Lost or Subsystem down, B:CTL blockade or Parts blockade, C:Minor issue

	No.	Class	Level	HDS Case No. ESC/CTSC/APSC	Problem ID	items	description	Official Release: Release Date	Official Release: ECN	Official Release: FCB
						V3.2/E, 0832/E		5/22/2008	002	-
V3.2/E, 0832/E	1	N	-		None	Support DF800	[Phenomena] Support DF800M/S			
						V3.2/G, 0832/G		6/20/2008	19	-
V3.2/G, 0832/G	1	C	B		V40QA076	HDD installation failure on Single mode or CTL blockade	[Phenomena] The HDD installation may fail in Dual mode with one CTL blockaded or Single mode. [Conditions of Occurrence] <In case of Dual mode > (1)HDD blockade (2)CTL blockade occurred before blockaded HDD repaired (3)New HDD is installed before recover CTL <In case of Single mode > (1)HDD is not installed in a slot (2)Install HDD into the slot in online. [Cause] When a HDD is inserted into a slot, HDD type is checked whether SAS or SATA. The HDD insertion fails in case of Dual mode with one CTL blockaded or Single mode because the HDD type may be			
	2	C	B		V40QA059	Shutdown may fail after a controller failure	[Phenomena] '- Shutdown may fail with a message "Microprogram error [FSM]", after PS OFF in a controller failure. - Shutdown may fail and stop without any message due to controller failure during PS OFF sequence [Conditions of Occurrence] When one of the following conditions is met, the phenomenon may occur. (1) PS OFF during a controller failure (2) Controller failure occurs during PS OFF sequence. [Cause] Due to the firmware bug, during PS OFF sequence, unexpected status may occur due to the misalignment between hardware			
	3	C	B		V40QA052	Invalid controller failure may occur on TrueCopy/TCED	[Phenomena] Following failure may occur, after controller failure occurs in the local site of True Copy/TCED. - Another controller failure may occur in the local site then subsystem goes down. - A controller failure may occur in the remote site. - PAIR status may not be changed (still old) [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (1) during PAIR or COPY status of TrueCopy/TCED (2) controller failure occurs in the local site [Cause] Due to the firmware bug on the TrueCopy/TCED, copy status may			
	4	C	B		V40QA082	Pair operations, such as splitting, swapping, and deleting from S-VOL, may fail when the maximam number of supported remote replication pairs is not equal with the paired unit.	[Phenomena] Pair operations such as splitting, swapping, and deleting from S-VOL, may fail when the maximam number of supported remote replication pairs, on TrueCopy Remote Replication or TrueCopy Extended Distance, is not equal with paired unit.. In case of CCI, the following codes are generated. Sense Key/Code(Detail) = 5/961C(0018) or 5/961C(0019) In case of HSNM2, the following error messages are generated. DMER080018: The LUN of the P-VOL is higher than 512 (1023). Make sure of the number of the specified paired LU. DMER080019: The LUN of the S-VOL is higher than 512 (1023). Make sure of the number of the specified paired LU. [Conditions of Occurrence] <used to do pair operations by HSNM2> A. If all of the following conditions are met, splitting pair may fail. a. The LUN for S-VOL is over the maximam number of replication pairs supported on the unit where P-VOL resides. b. Split pair is executed. B. If all of the following conditions are met, swapping pair may fail. a. The LUN for P-VOL is over the max number of replication pairs supported on the unit where S-VOL resides. b. Swap pair is executed. If all of the following conditions are met, swapping pair may fail. C. If all of the following conditions are met, deleting pair from S-VOL will fail.			
						V4.0, 0840/A		6/16/2008	017	-
	1	N	-		None	Support DF800H	Support DF800H			
	2	N	-		None	Support SSL	Support SSL			
	3	N	-		None	Support TC/TCE of DF800H - DF800M/S and DF700	Support TC/TCE of DF800H - DF800M/S and DF700			

	4	N	-		None	Support BCC setting for E-mail	Support BCC setting for E-mail
	5	N	-		None	Support offline upgrade (DF800S -> DF800M)	Support offline upgrade (DF800S -> DF800M)
	6	I	-		None	Improve response time of RAID1+0 for SPC-1	Improve response time of RAID1+0 for SPC-1
	7	C	B		V33-0091	Controller recovery failure after tuning on subsystem with an uninstalled controller.	[Phenomena] Controller recovery may fail, when controller is installed after tuning on subsystem with an uninstalled controller. [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (1) Turning on subsystem with a controller uninstalled. (2) Installing controller after subsystem READY. [Cause] Due to a firmware bug, controller uninstalled status was wrongly kept, and subsystem failed controller recovery with the status.
	8	C	B		V33-S036	PIN over after controller or backend failure	[Phenomena] PIN over may occur after controller failure or backend failure. [Conditions of Occurrence] This failure may occur when intermittent hardware failure occurs on the controller or backend. [Cause] Due to the firmware bug, HDD access was wrongly stopped after intermittent hardware failure on the controller or backend.
	9	C	C		V40-0214	Unreasonable U.A. (Unit attention) factor reset after online firmware update	[Phenomena] Factor of U.A. (Unit attention) may be unreasonably cleared after online firmware update. [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (1) Subsystem keeps U.A. factor. (2) executing online firmware update. [Cause] Due to a firmware bug, U.A. factor was not took over during online firmware update process.
	10	C	B		V40QA052	Controller failure after another controller failure on TrueCopy/TCED	[Phenomena] Following failure may occur, after controller failure occurs on the local site of True Copy/TCED. - failure of the other controller on the local site - another controller failure on the remote site. - PAIR status may not be changed [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (1) during PAIR or COPY status of TrueCopy/TCED (2) controller failure occurs [Cause] Due to firmware bug on the TrueCopy/TCED, copy status got wrong value after controller failure.
	11	C	B		HHARD074	Unreasonable ENC/HDD/Controller failure after hardware failure of backend or controller	[Phenomena] ENC/HDD/Controller may be unreasonably failed (blocked) after hardware failure on then backend line or on a controller. [Conditions of Occurrence] When some one of the following conditions are met, the phenomenon may occur. (1) Frame failure on the backend line (2) intermittent failure on a controller [Cause] Due to the firmware bug, firmware blocked wrong FRU part that differs from actual failure part.
	12	C	B		V40QA059	Shutdown failure after a controller failure	[Phenomena] - Shutdown may be failed with a message "Microprogram error [FSM]", after PS OFF during a controller failure. - Shutdown may be failed and stopped without any message, after controller failure during PS OFF sequence. [Conditions of Occurrence] When some one of the following conditions are met, the phenomenon may occur. (1) PS OFF during a controller failure (2) Controller failure occurs during PS OFF sequence. [Cause] Due to a firmware bug on the PS OFF sequence, firmware got unexpected status because of the misalignment between controllers.
	13	C	B		V40QA082	Pair operations such as splitting, swapping, and deleting from S-VOL, fail if the arrays whose max number of supported remote replication pairs are not the same.	[Phenomena] Pair operations such as splitting, swapping, and deleting from S-VOL, fail if the arrays whose max number of supported remote replication pairs, TrueCopy Remote Replication or TrueCopy Extended Distance, are not the same. In case of CCI, the following codes are generated. Sense Key/Code(Detail) = 5/961C(0018) or 5/961C(0019) In case of HSNM2, the following error messages are generated. DMER080018: The LUN of the P-VOL is higher than 512 (1023). Make sure of the number of the specified paired LU. DMER080019: The LUN of the S-VOL is higher than 512 (1023). Make sure of the number of the specified paired LU.

V4.0, 0840/A Base System V3.2/E, 0832/E						[Conditions of Occurrence] <If HSNM2 is used to do pair operations> A. If all of the following conditions are met, splitting pair will fail. a. The LUN for S-VOL is over the max number of replication pairs supported by the array where P-VOL resides. b. Split pair is executed. B. If all of the following conditions are met, swapping pair will fail. a. The LUN for P-VOL is over the max number of replication pairs supported by the array where S-VOL resides. b. Swap pair is executed. If all of the following conditions are met, swapping pair will fail. C. If all of the following conditions are met, deleting pair from S-VOL will fail. a. The LUN for P-VOL is over the max number of replication pairs supported by the array where S-VOL resides. b. Delete pair is executed at the array where the S-VOL resides. <If CCI is used to do pair operations> D. If all of the following conditions are met, pairsplit command will fail. a. The LUN for S-VOL is over the max number of replication pairs supported by the array where P-VOL resides. b. Pairsplit is executed. E. If all of the following conditions are met, pairsplit -R command [Cause] When remote replication pair operations such as splitting, swapping, and deleting from S-VOL, are tried, microcode is supposed to check only the LUNs within the array whether they are equal to less than the max number. But, the microcode incorrectly checks the following cases, too. When splitting pair, it checks whether the S-VOL is equal to or less than max number. When swapping pair, it checks whether the P-VOL is equal to or less than max number. When deleting pair from the S-VOL, it checks whether P-VOL is equal to or less than max number.
	14	C	B		V40-B004		[Phenomena] I/O error after backend or controller failure during online firmware update [Conditions of Occurrence] Following failure might occur after backend or controller failure during online firmware update. - Host I/O timeout - HDD or controller might be wrongly blocked that differs from actual failure part. [Cause] When all of the following conditions are met, the phenomenon may occur. (1) during online firmware update (2) backend or controller failure
	15	C	C		V40QA001	Wrong message display during host I/O	[Phenomena] Following wrong message may be displayed, when subsystem receives host I/O on the RAID group that contains 15 HDDs or more for DF800M, or 10 HDDs or more for DF800S. "Drive response diagnosis detected the slowdown of HDU I/O performance" [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (1) receiving host I/O onto the RAID Group that contains 15 HDDs or more for DF800M, or 10 HDDs or more for DF800S (2) Ready (No warning) [Cause] Due to a firmware bug, HDD's response information was wrongly updated during host I/O.
	16	C	B		HDS-068	No failback after FC cable pull-out on local port of the TrueCopy	[Phenomena] No failback might be executed on the remaining TrueCopy path, if FC cable on the Remote site is pulled-out and put-in, after Local site FC cable pull-out/put-in. [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (1) using TrueCopy/TCED (2)pulling-out and putting-in the FC cable on to the Local port. (3) pulling-out and putting-in the FC cable on to the Remote port. [Cause] Due to a firmware bug, subsystem modified status wrongly on the local site, and cause FC path recovery failure on the Remote site.
	17	C	C		V40-0226	Wrong E-mail messages	[Phenomena] Following wrong E-mail message might be sent via E-mail Alert. - Wrong firmware version after firmware update - Wrong device type - Wrong hardware serial number - Wrong host I/F model [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (1) using E-mail Alert (2)E-mail is sent with some failure. [Cause] Due to a firmware bug, firmware referred wrong information to

	18	C	B		V40QA076	HDD installation failure on Single mode or CTL blockade	[Phenomena] The HDD installation in the slot fails in Dual mode with one CTL blockaded or Single mode. [Conditions of Occurrence] <In case of Dual mode > A. HDD blockade B. CTL blockade occurred before HDD recovery C. Recover CTL before HDD recovery <In case of Single mode > A. HDD is not installed in a slot B. Install HDD into the slot in online. [Cause] When a HDD is inserted into a slot, the firmware checks HDD type, SAS or SATA. The HDD insertion fails in case of Dual mode with one CTL blockaded or Single mode because the firmware recognizes illegal HDD type by firmware bug.	
	19	C	B		V40QA061	LA/LRC error after controller failure	[Phenomena] Following failure might occurs, if controller failure occurs with CPU halt. " LA/LRC error was detected" or "Target abort INT status error" [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (1) High workload with Write I/O (2) Controller failure with CPU halt [Cause] SAS controller chip transferred wrong date to the drive after CPU halt.	
	20	C	B		V33-B031	I/O error after the intermittent failure during controller recovery	[Phenomena] I/O error might occur when intermittent failure occurs during controller recovery [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (1) during controller recovery (2) intermittent failure [Cause] Due to a firmware bug on the timeout threshold, I/O error might occur after the intermittent failure during controller recovery.	
	V4.3, 0843/B							7/15/2008	020 -
	1	N	-		None	Support DF800 M/S iSCSI	Support DF800 M/S iSCSI		
	2	N	-		None	Support TC/TCE of DF800 M/S iSCSI	Support TC/TCE of DF800 M/S iSCSI		
	3	N	-		None	Support offline upgrade (DF800S or DF800M -> DF800H)	Support offline upgrade (DF800S or DF800M -> DF800H)		
	4	I	C	SD2165969	DF700-52672	Improve message of Q-Full occurrence	Improve message of Q-Full occurrence		
	5	I	C		None	Improve sequential read performance in Quick format	Improve sequential read performance in Quick format		
	6	I	C	SD2189607	None	Improve sequential read performance at crosscall I/O.	Improve sequential read performance at crosscall I/O.		
	7	C	B		V43-0004	After the model upgrade was executed, the remote copy path failed.	[Phenomena] After the model upgrade was executed, the remote copy path failed. [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (1) A remote copy is used. (2) The offline upgrade from DF800S to DF800M is executed. [Cause]		
	8	C	A		V43-0068	When the failure of the another CTL is occurred, Micro program Error [RSM] is generated.	[Phenomena] When the failure of the another CTL is occurred, Micro program Error [RSM] is generated. [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (1) DF800H (2) When the failure of the another CTL is occurred. [Cause] The lock processing between controllers passes each other by processing that executes the recovery of the failure. As a result, the state of logical contradiction is occurred because the state of the		
	9	C	A		V43-B008	After the controller had replaced, the host I/O stopped.	[Phenomena] When the other controller is inserted in the equipment to stand up as a single controller, the host I/O stops. [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (1)Equipment to stand up as single controller (2)When equipment starts up, one controller fails. Afterwards the controller recovers by replace operation or the controller's auto rebooting. (3)When equipment starts up, one controller fails. Afterwards the controller recovers by replace operation or the controller's auto rebooting. [Cause] The table couldn't initialize, because the table initialization was		
	10	C	B		V43-B005	The communication time-out is generated while the state transition of TC is occurred.	[Phenomena] The communication time-out is generated when the state transition of TC operates while executing host's I/O, and controller failure is occurred. [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (1) during PAIR or COPY status of TrueCopy/TCED (2)controller failure occurs in the local site [Cause]		

V4.3, 0843/B Base System V4.0/A, 0840/A	11	C	B		V43-0056	After the controller had generated reset, the controller failure was generated.	[Phenomena] After the controller had generated reset, the controller failure was generated. [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (1) The controller had generated reset. (2) The I/O load is heavy. [Cause]		
	12	C	B		V43-0057	The subsystem is downed by the controller failure in host I/O.	[Phenomena] Microprogram error [DSC] is generated in another controller when the controller failure is occurred while processing host I/O and the subsystem is downed. [Conditions of Occurrence] The controller failure is occurred. [Cause] When the controller failure is occurred, the processing of		
	13	C	B		V43-B011	The HDD blockage by unjustified LA error is generated.	[Phenomena] When the uncorrectable error is detected in online verify, HDD is blockaded by detecting an unjustified LA error. [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (1) Online verify is operating. (2) RAID6 (3) The uncorrectable read error is detected. [Cause] Because the microprogram accesses an illegal address area by the		
	14	C	B		V43-0089	When the controller is blockaded, host I/O, HSNM2, and the Web console connection cannot be connected.	[Phenomena] When the uncorrectable error is detected in online verify, HDD is blockaded by detecting an unjustified LA error. [Conditions of Occurrence] The controller is blocked. [Cause] When the controller is blockaded, host I/O, HSNM2, and the Web console connection cannot be connected. Because interrupt is masking done unjustified by the recovering processing when		
	15	C	B		V43-0087	The pool setting ends normally even if there is lack of the table that manages the capacity of the pool.	[Phenomena] When the uncorrectable error is detected in online verify, HDD is blockaded by detecting an unjustified LA error. [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (1) A set instruction of the pool volume was received exceeding the capacity of the pool that was able to be managed. (2)The user tries to register the volume of 32LU or more in the volume of the pool at a time. [Cause] Because microprogram did not check whether the volume since		
	16	C	B		V43-0091	After microprogram exchange, the write through mode becomes improper.	[Phenomena] After the microprogram exchange with the write through mode setting, the write through mode is turned off. [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (1) The write through mode is turned ON. (2) After microprogram exchange is executed. (3) The battery alarm is occurred. [Cause] When CTL exchange/rebooting/no stop microexchange is executed with the battery alarm generated, the write through cannot operate because there is no opportunity when the write		
	17	C	B		V45-0006	When equipment starts up, the equipment can not stand up in the composition where SAS HDDs are maximum mounted.	[Phenomena] When equipment starts up, the equipment can not stand up in the composition where SAS HDDs are maximum mounted. [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (1)DF800H (2)SAS HDDs are mounted with 31 or 32 RKAKs. [Cause] When the SAS disks are mounted with 31RKAKs or 32RKAKs, the recognized processing of SAS disks fails by microprogram error.		
	V4.5, 0845/A							7/31/2008	029 -
V4.5, 0845/A Base System V4.3/B, 0843/B	1	N	-		None	Support 4GB cache DIMM.	Support 4GB cache DIMM.		
	2	C	A		V45QA003	Watch-dog timeout error occurred with pair delete operation, during MPU failure.	[Phenomena] The hardware error occurs by a CTL, a kernel processing error and Watch-dog time-out occur by a another CTL, and the subsystem is downed. [Conditions of Occurrence] (1)CTL failure is occurred (2)DF800H [Cause] The processing to match the synchronization between two cores		
	3	C	A		V45QA001	The system down is generated by failure of the power supply(3.3V) component.	[Phenomena] The system down is generated by failure of the power supply(3.3V) component. [Conditions of Occurrence] (1)Failure of the power supply(3.3V) component (2)The microprogram detects the time-out of the PCI bridge in the controller. [Cause] The microprogram mistakes the judgment condition of the failure factor, when the microprogram detects the time-out of the PCI		
	V4.3, 0843/C							9/26/2008	040 -

V4.3, 0843/C Base System V4.3/B, 0843/B	1	N			None	Support QE4+ I/F board* for DF800M/H. *:PK Assy : SH482-B(Hardware will be relesed at 10/'08)	Fibre Channel I/F chip will be changed from QE4 to QE4+. The I/F board will QE4 to QE4+ be compatible	
	2	I			None	Integration of procedure for installing unique information to HDD	Installed information on each kind of HDD had been selected. To install unique information without the selection of the type of HDD, the procedure was changed.	
	3	C	A		V43-0099	LA error [DRR] occurred on CTL0 while CTL1 was recovered by dummy replacement.	[Phenomena] LA error [DRR] occurred on CTL0 while CTL1 was recovered by dummy replacement. [Conditions of Occurrence] (1)CTL's MPU failure is occurred (2)CTL dummy replacement [Cause] The header of cashe was broken by the failure of controller's MPU while gathering the trace. The trace was gathered and referring to the broken header after the dummy is replaced, the trace has been	
	4	C	B		V43-0095	The error log of Event ID6 is output on Windows OS at the test of server rebooting.	[Phenomena] The error log of Event ID6 is output on Windows OS at the test of server rebooting. [Conditions of Occurrence] (1)Cross path IO [Cause] There is a case for the threshold to improve unjustified counting when I/F controller's Freeze is executed. Linkinitialize is executed at threshold over time. Because OS detected the Linkup event unjustified, the log has	
	5	C	A		V43-0105	A non-stop microexchange is executed from V4.3/C to V4.6/A and the system is hung up.	[Phenomena] A non-stop microexchange is executed from V4.3/C to V4.6/A and the system is hung up. [Conditions of Occurrence] (1)CTL reboot [Cause] The kernel function was called when the system state flag was made READY when CTL was rebooted, and the information of the special process was not reflected in local memory. So CTL	
	6	C	A		V43QA014	The CTLfailure is generated by Micro program error [RCH].	[Phenomena] When SI resync was executed, the CTL failure was generated by Micro program error [RCH] while executing RD/WR IO processes. [Conditions of Occurrence] (1)DF800H (2)LU made in 1RG when LUs are mapping in each core. [Cause] Logical contradiction is generated by the middle dirty check,	
	7	C	A		-	For Errata of MPU	[Phenomena] After the controller had generated reset, the CTL failure was generated. [Conditions of Occurrence] (1)Initialize and rebbot [Cause]	
	8	C	A		HDS-083	CTL failure occurred when cross path IO is issued between CTL or cores in high load IOs	[Phenomena] CTL failure occurred when cross path IO is issued between CTL or cores in high load IOs [Conditions of Occurrence] (1)High load IOs (2)READ I/O operations of crose path IO of about 16KB in transfer length [Cause] When the high load IO operation were executed, the buffer on PCI were full by I/F controller and by the cross path register access, and detecting the time-out of PCI, CTL failure occurred by PCI	
	9	C	A		V43-0110	ENC failure and systemdown occurred with the IO operation ENC microexchage, LU switch , and the format tests.	[Phenomena] ENC failure and systemdown occurred with the IO operation ENC microexchage, LU switch , and the format tests. [Conditions of Occurrence] (1) LU switch (LU load balance) or cashe Directory switch operation(controller blockage and micro exchange) (2) Under the condition 1, initialization process and the another side's CSDS write operation crossed each other. (3) Under the condition 2, the initialization of the flag in another CTL side core is executed. [Cause] When LU is switch ed, the flag in 0Y core is cleared by the microprogram bug and the response is not returned to demand origin core of LU switch . Therefore, 1X core keeps waiting for	
	10	C	A		V43-0121	The pinover occurred with host IO and ENC microexchange.	[Phenomena] The pinover occurred with host IO and ENC microexchange. [Conditions of Occurrence] (1)CHK1 occurres [Cause] When CHK1 was generated, the flag executing JOB of each PATH number had not been turned off and HDD device discovery operation was not executed. Therefore, all device reset piled up in concerned PATH, the PDEV time-out happened frequently, and Pinover occurred.	
	11	C	A		V43-0117	The CTL failure was generated while sequential WR IO operation was executed.	[Phenomena] The CTL failure was generated while sequential WR IO operation was executed. [Conditions of Occurrence] (1)CHK1 occurres [Cause] The deadlock of PCI is generated by LSI ASIC of DF, and the CTL failure occurred.	

	12	C	A		V43-0098	Watch-dog timeout error occurred with pair delete operation during MPU failure.	[Phenomena] Watch-dog timeout error occurred with pair delete operation during MPU failure. [Conditions of Occurrence] (1)DF800H (2)CTL failure occurres [Cause] The hardware error occurs by a CTL, a kernel processing error and Watch-dog time-out occur by a another CTL, and the			
	13	C	A		V43-0096	The system down is generated by failure of the power supply(3.3V) component.	[Phenomena] The system down is generated by failure of the power supply(3.3V) component. [Conditions of Occurrence] (1)Failure of the power supply(3.3V) component (2)When condition 1. is generated, the microprogram detects the time-out of the PCI bridge in the controller. [Cause] The microprogram mistakes the judgment condition of the failure factor when the microprogram detects the time-out of the PCI			
	14	C	A		HDS-081, 085	Pinover occurred	[Phenomena] Pinover occurred [Conditions of Occurrence] (1)DF800H (2)High load IO [Cause] The cross IOs between cores is waited for executing temporarily because of full of internal IO que. In this case, the change of the order of the que is generated, the command sinks. As a result, the			
	V4.6, 0846/A							9/26/2008	041	-
V4.6, 0846/A Base System V4.5/A, 0845/A	1	N	-		None	Improving I/O Response Time In Small-Scale Configuration	Improving I/O Response Time In Small-Scale Configuration			
	2	N			None	Support QE4+ I/F board* for DF800M/H. *:PK Assy : SH482-B(Hardware will be relesed at 10/'08)	Fibre Channel I/F chip will be changed from QE4 to QE4+. The I/F board will QE4 to QE4+ be compatible			
	3	C	A		V46QA001	LA error [DRR] occurred on CTL0 while CTL1 was recovered by dummy replacement.	[Phenomena] LA error [DRR] occurred on CTL0 while CTL1 was recovered by dummy replacement. [Conditions of Occurrence] (1)CTL's MPU failure is occurred (2)CTL dummy replacement [Cause] The header of cashe was broken by the failure of controller's MPU while gathering the trace. The trace was gathered and referring to the broken header after the dummy is replaced, the trace has been			
	4	C	B		V46-0008	The error log of Event ID6 is output on Windows OS at the test of server rebooting.	[Phenomena] The error log of Event ID6 is output on Windows OS at the test of server rebooting. [Conditions of Occurrence] (1)Cross path IO [Cause] There is a case for the threshold to improve unjustified counting when I/F controller's Freeze is executed. Linkinitialize is executed at threshold over time. Because OS detected the Linkup event unjustified, the log has			
	5	C	A		V46QA005	A non-stop microexchange is executed from V4.3/C to V4.6/A and the system is hung up.	[Phenomena] A non-stop microexchange is executed from V4.3/C to V4.6/A and the system is hung up. [Conditions of Occurrence] (1)DF800H (2)CTL reboot [Cause] The kernel function was called when the system state flag was made READY when CTL was rebooted, and the information of the special process was not reflected in local memory. So CTL			
	6	C	A		V46-0013	The CTL blockage is generated by Micro program error [RCH].	[Phenomena] When SI resync was executed, the CTL blockage was generated by Micro program error [RCH] while executing RD/WR IO processes. [Conditions of Occurrence] (1)DF800H (2)LU made in 1RG when LUs are mapping in each core. [Cause] Logical contradiction is generated by the middle dirty check,			
	7	C	A		-	The controller failure occurred at PS ON.	[Phenomena] The controller failure occurred at PS ON. [Conditions of Occurrence] (1)Initialize and rebbot [Cause] CPU detected internal bus failure.			
	8	C	A		HDS-083	CTL failure occurred when cross path IO is issued between CTL or cores in high load IOs	[Phenomena] CTL failure occurred when cross path IO is issued between CTL or cores in high load IOs [Conditions of Occurrence] (1)DF800H (2)High load IOs (3)READ I/O operations of crose path IO of about 16KB in transfer length [Cause] When the high load IO operation were executed, the buffer on PCI were full by I/F controller and by the cross path register access,			

	9	C	A		V46-0020	ENC failure and systemdown occurred with the IO operation ENC microexchage, LU switch , and the format tests.	[Phenomena] ENC failure and systemdown occurred with the IO operation ENC microexchage, LU switch , and the format tests. [Conditions of Occurrence] (1) LU switch (LU load balance) or cashe Directory switch operation(controller blockage and micro exchange) (2) Under the condition 1, initialization process and the another side's CSDS write operation crossed each other. (3) Under the condition 2, the initialization of the flag in another CTL side core is executed. [Cause] When LU is switch ed, the flag in 0Y core is cleared by the microprogram bug and the response is not returned to demand origin core of LU switch . Therefore, 1X core keeps waiting for		
	10	C	A		V46-0018	The pinover occurred with host IO and ENC microexchange.	[Phenomena] The pinover occurred with host IO and ENC microexchange. [Conditions of Occurrence] (1)CHK1 occurres [Cause] When CHK1 was generated, the flag executing JOB of each PATH number had not been turned off and HDD device discovery operation was not executed. Therefore, all device reset piled up in concerned PATH, the PDEV time-out happened frequently, and		
	11	C	A		V46QA007	The CTL failure was generated while sequential WR IO operation was executed.	[Phenomena] The CTL failure was generated while sequential WR IO operation was executed. [Conditions of Occurrence] (1)CHK1 occurres [Cause] The deadlock of PCI is generated by LSI ASIC of DF, and the CTL failure occurred.		
	12	C	A		V46-0015	Pinover occurred	[Phenomena] Pinover occurred [Conditions of Occurrence] (1)DF800H (2)High load IO [Cause] The cross IOs between cores is waited for executing temporarily because of full of internal IO que. In this case, the change of the order of the que is generated, the command sinks. As a result, the		
	13	C	A		V46-0027	A CTL failure is generated by Micro program error [POM]/[SNR].	[Phenomena] A CTL failure is generated by Micro program error [POM]/[SNR]. [Conditions of Occurrence] (1) Pairs of SnapShot or TrueCopy Extended Distance exist. (2)Hosts are executing I/O to the pairs or SnapShot restoring is executing (3) Single CTL failure has occurred. (4)Ownership of a LU that is not belong the pairs defined by condition 1 and 2. Even if the CTL failure has occurred, it is possible to change the LU ownership because microcode manages which CTL owns the LUs in each CTL. [Cause] When single CTL failure has occurred, the table on memory is abnormally updated because of the conflict of the process of data copy and changing ownership of a LU. As a result		
	14	C	A		V46QA013	When the ENC was pulled out and was inserted, the subsystem-down was generated by both of controllers' failure.	[Phenomena] When the ENC was pulled out and was inserted, the subsystem-down was generated by both of controllers' failure. [Conditions of Occurrence] (1) Seqential write IOs (2) High load IOs (3) The data transfer length is about 16 KB. [Cause] The cross IOs between cores is waited for executing temporarily because of full of internal IO que. In this case, the change of the order of the que is generated, the command sinks. As a result, the		
					V4.6, 0846/B			10/14/2008	050	4
V4.6, 0846/B Base System V4.6/A, 0846/A	1	C	A		V46-0034	Data reliability improvement	[Phenomena] "Data transfer length inconsistency error" in a write operation to a SAS HDD, causing possible data inconsistency. [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (a) The SAS HDD has some unstable behavior and "Data transfer length inconsistency error" occurs in the SAS HDD. (b) The SAS HDD responds normal end condition without the data transfer error. RSD considers that the occurrence rate is very low, because RSD has never experienced such a failure phenomenon ever before. [Cause] Due to the microcode bug in the recovery process for "Data transfer length inconsistency error" in the write operation to an		
	2	C	A		V46-0035	The I/O error occurs by LU switch + I/O operation.	[Phenomena] The I/O error occurs by LU switch + I/O operation. [Conditions of Occurrence] 1. LU unit switch 2. SyncCache/ModeSelect command [Cause] The exclusion of the processing between controllers failed, because the LU unit switch and the SyncCache/ModeSelect command		
					V5.0, 0850/B			11/11/2008	056Rev1	5
V5.0, 0850/B Base	1	N	-		None	Support the external power supply for DF800H model	The external power supply for DF800H model is supported.			
	2	N	-		None	Support SAS 450GB HDD	SAS 450GB HDDs are supported			
	3	I	-		None	SATA performance	SATA write performance increasing			

System V4.6/B, 0846/B	4	C	B		V50-0017	HDD blockade or PIN over occurred when another HDU was blockaded	[Phenomena] HDD blockade or PIN over occurred when another HDU was blockaded [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (1) SATA HDD was blockaded (2) After that, the SATA HDD appears on the backend SAS route illegally. (3) After that, the SATA HDD disappears on the backend SAS route illegally. (4) Atrer that (2) and (3) repeat continuously. [Cause] Due to the firmware bug, firmware searches the blockaded SATA HDD illegally. Then normal I/O was prevented by the serch traffic.
	5	C	B		V50-0082	Controller is blockaded with "Microprogram error[FSM]" when CHK1 reset occurs	[Phenomena] Controller is blockaded with "Microprogram error[FSM]" when CHK1 reset occurs The message "Microprogram error[FSM]" is displayed. [Conditions of Occurrence] The problem may occur when CHK1 reset occurs. [Cause] Due to the firmware bug, firmware sets illegal value to memory.
	6	C	B		V50-0089	Illegal HDD or ENC are blockaded when one controller is blockaded.	[Phenomena] Illegal HDD or ENC are blockaded when one controller is blockaded. [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) One controller is blockaded.
	7	C	B		V50-0111	Host I/O performance decreases when ENC firmware download is executed and controller was blockaded	[Phenomena] Host I/O performance decreases when ENC firmware download is executed and controller was blockaded [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) ENC firmware download is executed (2) One controller is blockaded. [Cause] Due to the firmware bug about ENC download process.
	8	C	B		V50-0128	Shutdown process stops in single controller configuration when HDD media error occurs	[Phenomena] Shutdown process stops in single controller configuration when HDD media error occurs [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Single controller configuration or Dual controller configuration with one controller blockaded (2) HDD media error occurs in shutdown process [Cause] Due to the firmware bug about shutdown process.
	9	C	B		V50-S014	PIN over occurred when ENC firmware download is executed	[Phenomena] PIN over occurred when ENC firmware download is executed [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Host I/O is executed. (2) ENC firmware download is executed. (3) SAS backend diagnostic process is executed because there is a failure part on SAS backend. [Cause] Due to the firmware bug about ENC download process.
	10	C	B		V50-B018	Controller is blockaded with "Microprogram error[CMD]" when Host I/O traffic is high	[Phenomena] Controller is blockaded with "Microprogram error[CMD]" when Host I/O traffic is high. The message "Microprogram error[CMD]" is displayed. [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Fibre Channel Host I/F (2) Host I/O traffic is high [Cause]
	11	C	B		V50-B030	Controller is blockaded with "Microprogram error[ISM]" when QLogic iSCSI HBA connects to DF/SA	[Phenomena] Controller is blockaded with "Microprogram error[ISM]" when QLogic iSCSI HBA connects to DF/SA The message "Microprogram error[ISM]" is displayed. [Conditions of Occurrence] The problem will occur when all following conditions are met. (1) iSCSI Host I/F (2) QLogic iSCSI HBA (3) Target number is equal or over 174 [Cause]
	12	C	A		V50QA037	Subsystem down in boot process occurs with ENC failure	[Phenomena] Subsystem down in boot process occurs with ENC failure [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) ENC hardware failure (2) Boot process [Cause] Due to the firmware bug about boot process.
	13	C	A		V50-0315	When the queue full status responds to host, the controller is blockaded.	[Phenomena] When the queue full status responds to host, the controller is blockaded. [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (a)High load (b)More than 1400 commands are received at the same time. (c)The queue full status responds [Cause] The lack of resources is generated by the internal resource defect when the response to the command from the server is delayed, and

	14	C	A		V50-0320	When the uncorrectable error of cache is occurred, an illegal message is output.	[Phenomena] When the uncorrectable error of cache is occurred, the web message reports on wrong cache slot number. [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (a) DF800M/H (b)The uncorrectable error of cache is occurred. [Cause]		
	15	C	A		V50QA051	ENC failure occurs when removing ENC_PK (or ENC cable)	[Phenomena] Removing ENC_PK (or ENC cable) from the operating DF800 causes other Expander's error (ENC failure). There is a few potential to occur Subsystem down finally. [Conditions of Occurrence] Removing the ENC_PK (or ENC cable) during transmitting write data to SATA-HDD with the other path, and Expander cannot transfer "Break", because Expander's resource is not released. [Cause] Current setting of Expander is to transfer "Break" via Expander's own FIFO. If Expander's resource (FIFO) is not released due to above condition, later access request is failed and results in the		
	V5.0, 0850/C							11/25/2008	074 -
V5.0, 0850/C Base System V5.0/B, 0850/B	1	C	A		V50-0326	Controller is blockaded when RST switch on another controller is pushed.	[Phenomena] Controller is blockaded when RST switch on another controller is pushed. [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) DF800H (2) Forced write through mode is valid. (3) A controller is blockaded. [Cause]		
	2	C	B		V50-0327	A controller failure occurs during subsystem booting.	[Phenomena] A controller failure occurs during subsystem booting. [Conditions of Occurrence] The problem occur whens all following conditions are met. (a) System Configuration A. Dual controller system B. System HDU is SATA HDU. C. One or more SATA HDUs are carried in RKAK. (b) Operations A. A subsystem is shut down. B. Power supply to RKA with one or more SATA HDUs is stopped and started again. C. Booting the subsystem. [Cause]		
	V5.2, 0852/A							11/25/2008	065 -
V5.2, 0852/A Base System V5.0, 0850/B	1	N	-		None	RG Expansion	RG Expansion is supported.		
	2	N	-		None	LU Grow/Shrink	LU Grow/Shrink and LU esay create are supported.		
	3	N	-		None	Online HDD firmware upgrade	Automatic online HDD firmware upgrade is supported.		
	4	N	-		None	Load Balancing Monitoring Time	Parameter of Monitoring Time for Load Balancing is added in System of Tuning Parameter.		
	5	C	B		V52-0103	DF800H cannot response Check Condition status if CHK1 reset occurs on the MPU core without the associated I/F board.	[Phenomena] DF800H cannot response Check Condition status if CHK1 reset occurs on the MPU core without the associated I/F board. Host recognizes the command issued to DF800H is timeout. [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (1) I/F board configuration; "0X/1X"= FibreChannel/None, or "0X/1X"= None/FibreChannel, or "0Y/1Y"= FibreChannel/None, or "0Y/1Y"= None/FibreChannel (2) Cross call access to MPU core without the associated I/F (3) CHK1 reset occurs on the MPU core without the associated I/F board [Cause] Due to the firmware bug about check condition response generation process.		
	6	C	B		V52-0135	Unit Attention is not respond to the host in iSCSI configuration	[Phenomena] Unit Attention(6/2900: Power On Reset) is not respond to the host in iSCSI configuration [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (1) A LU is deleted, and LU is generated whose internal LU# is same as previous deleted LU. (2) After (1) process, one of the conditions below occurs . - The host issued reset command. - CHK1 reset - Auto reboot - Shutdown and reboot - Firmware change (3) After (2) process, the host accesses to the LU. [Cause] Due to the firmware bug about Unit Attention(6/2900: Power On Reset) response generation process.		

	7	C	B		V52-S005	HSNM2 cannot be operated after LU deletion.	[Phenomena] HSNM2 cannot be operated after LU deletion. [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) A LU is deleted. (2) Host issues a command (FORMAT UNIT or SYNC CACHE or MODE SEL or WRITE BUFFER or P RESERVE OT or LAN SEL or Raid SEL) to deleted LU. (3) A LU is generated. [Cause] Due to the firmware bug, firmware cannot receive the command to HSNM2 for the operation.
	8	C	B		V52-0389	Illegal warning indication when LU is deleted during HDD warning status.	[Phenomena] Illegal warning indication when LU is deleted during HDD warning status. HDD warning status is cleared and HDD LED turns off. [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) During HDD warning status (2) LU delete or LU format or RG delete [Cause] Due to the firmware bug about warning status managing process.
	9	C	B		V52-0391	DF800 cannot respond any status to a host if a controller is blockaded or is during CHK1 reset.	[Phenomena] DF800 cannot respond any status to a host when Check Condition status should be responded if a controller is blockaded or is during CHK1 reset. [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) A controller is blockaded or is during CHK1 reset. (2) Check condition response for a command to a LU. The check condtion response occurs because of (1) status. (3) A command to the controller LU reset is received from the host during (2) process. [Cause] Due to the firmware bug about Check condition response generation process.
	10	C	B		V52-0396	Host I/O halts during 20 or more seconds when controller cannot issue the command through backend path during a few seconds	[Phenomena] Host I/O halts during 20 or more seconds when controller cannot issue the command through backend path during a few seconds [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Controller cannot issue the command through backend path during a few seconds because one of the conditions below occurs . - Backend path is blockadede - Link up NG - ENC firmware download - Backend diagnostic occurs - Backend Discover process (2) Special process (due to exclusive status between both controllers) is executed during condition(1) on both backend paths. [Cause] Due to the firmware bug about backend command issue process.
	11	C	B		V52-0393, V60-S006	HDD is blockaded illegally and a replaced controller doesn't reboot	[Phenomena] HDD is blockaded illegally and a replaced controller doesn't reboot [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) DF800H: two or more RKAs DF800M/DF800S: one or more RKAs (2) Controller is blockaded during one of the conditions below. - Online RKA adding. The added RKA has one or more SATA HDDs in it. - ENC insertion to RKA. The RKA has one or more SATA HDDs in it. - ENC firmware download. RKA that includes the ENC has one or more SATA HDDs in it - SATA HDD insertion (3) After (2) process, CTL replace is executed. [Cause] Due to the firmware bug about SATA HDD recognization in boot
	12	C	B		V52-0149	System Copy occurs in case of ENC failure	[Phenomena] System Copy occurs in case of ENC failure [Conditions of Occurrence] The problem may occur when ENC failure occurs in boot process. [Cause] Due to the firmware bug about boot process
	13	C	B		V52-0381	Controller is blockaded with "Microprogram error[BER]" when non stop firmware change is executed.	[Phenomena] Controller is blockaded with "Microprogram error[BER]" when non stop firmware change is executed. The message "Microprogram error[BER]" is displayed. [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) During non stop firmware change on one controller (2) Backend failure or illegal response from HDD occur on another controller [Cause] Due to the firmware bug about internal parameter setting.

	14	C	B		V52-0400, V60-0117	Online RKA adding is failed again after RKA adding failed	[Phenomena] Online RKA adding is failed again after RKA adding failed [Conditions of Occurrence] When all of the following conditions are met, the phenomenon may occur. (1) Online RKA adding is failed because ENC on the RKA is blockaded. (2) Then online RKA adding is executed to the same position as (1). [Cause] Due to the firmware bug about online RKA adding process.		
	15	C	B		V52-0405, V60-S009	Host I/O halts or HSNM2 cannot be operated when a controller is blockaded	[Phenomena] Host I/O halts or HSNM2 cannot be operated when a controller is blockaded [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) DF800H (2) One controller is blockaded. (3) At the timing of (2), another controller ececutes special process (due to exclusive status between both controllers). The Special process is related for HSNM2 operation. (4) At the timing of (2), blockaded controller executes synchronous process between MPU cores. [Cause] Due to the firmware bug about communication process between MPU cores.		
	16	C	A		V52-B024	Subsystem down occurs in Shadow Image copy process	[Phenomena] Subsystem down occurs in Shadow Image copy process [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Shadow Image copy is executed on a LU. (2) Shadow Image copy of other LU is completed on another controller. (3) Both controller refer the same table information on the memory simultaneously. [Cause] Due to the firmware bug about Shadow Image copy process.		
	17	C	B		V52-0406	Controller is blockaded when RST switch on another controller is pushed.	[Phenomena] Controller is blockaded when RST switch on another controller is pushed. [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) DF800H (2) Forced write through mode is valid. (3) A controller is blockaded. [Cause] Due to the firmware bug about Reset process		
	18	C	B		V52-0407	A controller failure occurs during subsystem booting.	[Phenomena] A controller failure occurs during subsystem booting. [Conditions of Occurrence] The problem occur whens all following conditions are met. (a) System Configuration A. Dual controller system B. System HDU is SATA HDU. C. One or more SATA HDUs are carried in RKA. (b) Operations A. A subsystem is shut down. B. Power supply to RKA with one or more SATA HDUs is stopped and started again. C. Booting the subsystem. [Cause] Due to the firmware bug about HDD recognization process during boot up.		
	19	C	B	D800-53333, EUC952882	None	CTL was blockaded when the setting of Cache Partition for Unified LU was changed.	[Phenomena] Controller is blockaded with following Web messages. Controller will not be recovered even though it is replaced by new controller as maintenance procedures. HJ0E15 Microprogram error[CMD] or HJ11D0 Microprogram error[RCH] [Conditions of Occurrence] The failure will occur when the followings conditions are met one by one. 1) LUs, whose Owner-CTL are different, are unified. 2) LU Ownership is changed caused by Load Balancing function. 3) The setting for LU location of Cache Partition is changed after above LU Ownership changing. [Cause] Because improper management information of Cache Partition for each LU is set when unified LU is created, Owner-CTL information for Main LU and Sub LU become inconsistent. Therefore, when this LU is accessed from host, the firmware detects self-contradiction error and the CTL is blockaded.		
						V5.0, 0850/D		12/26/2008	079	6
V5.0, 0850/D Base System V5.0/C, 0850/C	1	C	B		V50-0329	Random WriteI/O is slowing down with 2GB Cache on AMS2500.	[Phenomena] Random WriteI/O is slowing down with 2GB Cache on AMS2500. [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)AMS2500 (2) 2GB Cache (3)System including SATA HDD (4)Ramdom Write I/O [Cause]		

	2	C	A		V50-0332	I/O timeout caused by HDD failure at a change of configuration.	[Phenomena] I/O timeout caused by HDD failure at a change of configuration. [Conditions of Occurrence] The problem occur whens all following conditions are met. (1)Just before the following configurations change - A change of pair status for TrueCopy, ShadowImage, TCE and MVM - A creation/delete of RG/LU - A change of mapping - HDD blockade/recovery (2)A media error occurred during online verify process. [Cause] Microcode bug that current executing Jobs cannot be aborted while host I/Os are restrained at a process of a configuration	
	3	C	A		V50-0333	The timeout of IO commands occurred. As a result, a double HDD failure occurred and Pin-Over occurred.	[Phenomena] The timeout of IO commands occurred. As a result, a double HDD failure occurred and Pin-Over occurred. [Conditions of Occurrence] The problem occur whens all following conditions are met. (1) System including SAS HDD (2) Ratio between read and write data(read : write = 95:5 or over) [Cause] The traffic of read/write to the SAS interface responds to the response time of HDD. It increased priority to the read access. As a result, it takes long time to the write access, and the write access timeout occurs frequently. In addition, write access fails by the	
	4	C	A		None	WEB-SSL(443) port vulnerability	[Phenomena] Controller is blockaded with "Kernel Processing error". [Conditions of Occurrence] The problem occur whens all following conditions are met. (1)When web-HTTP(443)port access, SSL Hand Shake is running. (2)When it should be received "Client Hello"packet , it receive the other packet, or the connection is closed by FIN or RST	
	V6.0, 0860/A							12/28/2008 82
V6.0, 0860/A Base System V5.2, 0852/D	1	N	-		None	Dense Tray	Dense Tray is support	
	2	N	-		None	DF800H iSCSI	DF800H iSCSI is supoorted	
	3	N	-		None	IPv6	IPv6 is supported.	
	4	N	-		None	Discovery CHAP mode	Discovery CHAP mode is supported.	
	5	C	C		RKAKX015	PS_Alarm LED does not go out when (1) plural ENCs has blockaded but recovered and (2) PS recovered.	[Phenomena] When Plural ENCs and PS are blockaded, PS_Alarm_LED does not go out even after PS is exchanged. PS recovered message is issued normally. [Conditions of Occurrence] The problem occurs when all following conditions are met. (1) Hardware: DF800M/S/H + one or more external trays (2) Plural ENCs on the same backend path blockaded in short term (i.e. in 40 seconds). (3) The External Tray, which has the least Unit # among the External Trays including ENC blockaded in (2), also has other blockaded parts and a maintenance personnel exchanges the blocked parts	
	6	C	C		V60-0035	Permanent LinkUp NG occurs repeatedly after I	[Phenomena] Failure traces are recorded repeatedly after ENC has been blocked. [Conditions of Occurrence] The problem occurs when all following conditions are met. (1) LinkUP diagnostic is processing.. (2) In case of DF800H, an ENC in Unit#1, 2 or 3 is blockaded. In case of DF800M/S, ENC in Unit#1 is blockaded. (3) Until 1 minute after (2), Permanent LinkUp NG occurs repeatedly.	
	7	C	B		V60-0060	Wrong sort of reset to SAS Chip occurs.	[Phenomena] Host I/O cannot executed for several seconds. [Conditions of Occurrence] The problem occurs when all following conditions are met. (1) Hardware: DF800H (2) PCI Reset is executing in some backend path. (I.e. Power on cycle or some failure management processing) (3) In another backend path, Selective Reset request is received (I.e. other failure or ENC firmware download. [Cause]	
	8	C	B		V60-0116	Abnormal response to Cross LUN_Reset.	[Phenomena] Unable to detect the failure ENC. [Conditions of Occurrence] The problem occurs when all following conditions are met. (1) LUN reset to ENC is issued by cross-call. (2) The response to (1) is not "GOOD." [Cause]	
	9	C	B		V60-0121	IOCB timeout occurs during ENC firmware dov	[Phenomena] False blockade to ENC during ENC firmware download [Conditions of Occurrence] The problem occurs when all following conditions are met. (1) ENC blockade, ENC firmware download or ENC removal. (2) LUN Reset to the ENC is issued after (1). (3) Between (1) and (2), PHY disable or enable command is issued.	

	10	C	C		V60-0224	Correct IP address does not recorded in the Aud	[Phenomena] Wrong IP address is recorded in audit log when DHCP is on. (User setting value is recorded.) [Conditions of Occurrence] The problem occurs when all following conditions are met. - DHCP ON - Audit log is recorded. - IP address assigned by DHCP and IP address assigned by user is different [Cause] Due to the firmware bug about control/diagnostic command	
	11	C	B		V60-0250	Wrong CTL is blockaded when CTL error threshold is over on the crosscall in some CTL.	[Phenomena] Some CTL error threshold is over on the crosscall in some CTL. Then, the other CTL is blockaded. [Conditions of Occurrence] The problem occurs when all following conditions are met. (1) Dual CTL (2) Cross-call is executing among CTLs (3) Some CTL error threshold is over on the crosscall in some CTL. [Cause]	
	12	C	B		V60-0272	CHK1 occurs when parameters on E-Mail are c	[Phenomena] Setting E-mail parameters by SNM2 is unavailable. [Conditions of Occurrence] The problem occurs when all following conditions are met. (1) E-Mail parameter configuration setting/change/clear operation by HSMN2 (2) CHK1 occurs in the corresponding CTL at that time. [Cause] Due to the firmware bug about E-mail processing.	
	13	C	B		V60-B005	CTL with FC cable cannot recover when the CT	[Phenomena] Plugged-in CTL is blockaded by "communication send time-out" [Conditions of Occurrence] The problem occurs when all following conditions are met. 1. Front-end: FC interface 2. Online plug-in the CTL/PS-OFF/PS-ON/online firmware update 3. Link failure occurs in several seconds. [Cause]	
	14	C	B		V60-B009	Controller is blockaded by Microprogram error[ISM], during SnapShot command execution.	[Phenomena] Microprogram error[ISM] occurs and CTL is blockaded when SnapShot pair settings during host I/O operations. [Conditions of Occurrence] The problem occurs when all following conditions are met. (1) Hardware: iSCSI I/F (2) host I/Os to plural CPUs comes to one iSCSI port (3) SnapShot is executed during other I/O operation (4) Refresh of SnapShot information is slow (more than 500ms) [Cause] Due to the firmware bug about iSCSI driver.	
	15	C	B		V60-QA030	Due to ENC Linkup delay, other ENC is blocka	[Phenomena] ENCs may be blockaded falsely when ENC firmware download or ENC blockade. Following messages are displayed in that cases. I5H000 Backend link error was detected(Unit-06,ENC-0) W0FA00 ENC alarm(Unit-06,ENC-0) :ENC /STR [Conditions of Occurrence] The problem occurs when all following conditions are met. 1. Partial retry occurs in Discover. 2. The result of the retry is GOOD or Reject. 3. Linkup of ENC is slow. [Cause] Due to the firmware bug about SAS management.	
	16	C	B		V60-S011	IP address of maintenance port CTL1 is not correct when CTL0 is blockaded.	[Phenomena] The address of the maintenance port of CTL1 is displayed as [0.0.0.1](IPv4) and [::1](IPv6), on referring the address after blockade of CTL0. [Conditions of Occurrence] The problem occurs when all following conditions are met. (1) CTL#0 is blockaded (2) Thru CTL#1's LAN port, issue CLI command to display the IP address of maintenance port. Or, Thru CTL#1's LAN port, open GUI page that display the IP address of maintenance port. [Cause] Due to the firmware bug about control/diagnostic command	

V6.0, 0860/B Base System V6.0, 0860/A	1	C	B		V62-0021	Subsystem down on the Remote Array with "MicroProgram Error[POM]" after TCE pair is created.	[Phenomena] Create TCE pair (as P-Vol:LUN0, S-Vol:LUN1), then after the initial copy, Microprogram error[POM] occurs on the remote DF. (One CTL is blockaded in the DF and the DF become subsystem down. In the local DF, the pair creation fails and the TCE pair become PSUE.) [Conditions of Occurrence] When all following conditions (1)to(6) are met, either (A) or (B) will occur (A) A remote DF will become subsystemdown (B) Pair status will become PSUE. (Error in RG Expansion falsely) (1) Local DF: DF800 or DF700 (2) Remote DF: DF800 (3) TCE PP is available in both local/remote DF (4) LUN0 in the remote DF is not formed a pair of SnapShot or TCE (5) Except for LUN0 in the remote DF, TCE pair is created. When all following conditions (1)to(6) are met, either (A) or (B) will occur (B) Pair status will become PSUE. (Error in RG Expansion falsely) (1) Local DF: DF800 or DF700 (2) Remote DF: DF800 (3) TCE PP is available in both local/remote DF (4') LUN0 in the remote DF is formed a pair of SnapShot or TCE. And the pair status is PAIR(SS) or PSUS(TCE).	
	2	C	B		V60QA026	[RKH+Dense]HDU is blockaeded on the heatrun of I/O and ENC firmware download.	[Phenomena] (Config: RKH+Dense) LUN error is occurred on the heatrun of I/O and ENC firmware download. Then Message "IY1600 LA/LRC error was detected" is displayed and an HDU is blockaded. [Conditions of Occurrence] The problem occurs when all following conditions are met. (1) DF800H (2) Link Reset occurs in one of backend path 2/3, which is controlled by processor core Y. (Such link reset will be caused by SAS chip failure/ ENC failure/ ENC replace/ download of ENC firmware) (3) ID of HDU is changed on the backend discovery after the link reset of (2). (Such change will be caused by failure or configuration change on the backend.) (4) I/O is going to be issued to a HDU in the polling process (every 10 micro seconds) of processor core Y. In this I/O, the old ID of HDU is used. (5) In the same polling process of (4) (i.e. within 10 microseconds), in core X, the management table of HDU ID is refreshed based on the discovery. Thus I/O of (4) is processed though its ID is not same to (3)(5). [Cause]	
	3	C	B		V61-B009	Reboot of online firmware upgrade doesn't complete, and the other ("READY" state) controller cannot execute I/Os	[Phenomena] Reboot of online firmware upgrade doesn't complete, and the other ("READY" state) controller cannot execute I/Os [Conditions of Occurrence] The problem occurs when all following conditions are met. 1. DF800H 2. Execute online firmware update. (This issue doesn't occur when updating firmware with PS-OFF/ON.) 3. The Controller (which is READY) executes ModeSel or Persistent Reserve SCSI Command from host computers. The "Ready" controller processes the command as a synchronous processing (5 mili secomds). Such command will be sent from HP-UX or AIX when they re-recovnize devices. 4. Other controller processes the reboot process of online firmware update as a synchronous processing (30 mili seconds). If this processing occurs during (4), the issue will occur. [Cause]	
	4	C	C		V61-QA005	ENC is blockaded falsely when changing HDUs during I/O heatrun and SI copy.	[Phenomena] ENC is blockaded falsely when echanging HDUs during I/O heatrun and SI copy. Then I/Os are not processed. [Conditions of Occurrence] When backend diagnostics logic executes loopback diagnostics in HDD PHY, the PHY become disable by the blockade of HDU etc. [Cause] Due to the firmware bug about backend diagnostics.	
	V5.0, 0850/E							1/23/2009　90　-

V5.0, 0850/E Base System V5.0/D, 0850/D	1	C	B		V60QA026	HDU is blockaeded on the heatrun of I/O and ENC firmware download.	[Phenomena] LUN error is occurred on the heatrun of I/O and ENC firmware download. Then Message "IY1600 LA/LRC error was detected" is displayed and an HDU is blockaded. [Conditions of Occurrence] The problem occurs when all following conditions are met. (1) DF800H (2) Link Reset occurs in one of backend path 2/3, which is controlled by processor core Y. (Such link reset will be caused by SAS chip failure/ ENC failure/ ENC replace/ download of ENC firmware) (3) ID of HDU is changed on the backend discovery after the link reset of (2). (Such change will be caused by failure or configuration change on the backend.) (4) I/O is going to be issued to a HDU in the polling process (every 10 micro seconds) of processor core Y. In this I/O, the old ID of HDU is used. (5) In the same polling process of (4) (i.e. within 10 microseconds), in core X, the management table of HDU ID is refreshed based on the discovery. Thus I/O of (4) is processed though its ID is not same to (3)(5). [Cause] Due to the firmware bug about backend SAS management.	
	2	C	B		V61-B009	Reboot of online firmware upgrade doesn't complete, and the other ("READY" state) controller cannot execute I/Os	[Phenomena] Reboot of online firmware upgrade doesn't complete, and the other ("READY" state) controller cannot execute I/Os [Conditions of Occurrence] The problem occurs when all following conditions are met. 1. Execute online firmware update. (This issue doesn't occur when updating firmware with PS-OFF/ON.) 2. The Controller (which is READY) executes ModeSel or Persistent Reserve SCSI Command from host computers. The "Ready" controller processes the command as a synchronous processing (5 mili seconds). Such command will be sent from HP-UX or AIX when they re-recognize devices. 3. Other controller processes the reboot process of online firmware update as a synchronous processing (30 mili seconds). If this processing occurs during (4), the issue will occur. [Cause]	
	3	C	B		V60-QA030	Due to ENC Linkup delay, other ENC is blockaded falsely.	[Phenomena] ENCs may be blockaded falsely when ENC firmware download or ENC blockade. Following messages are displayed in that cases. "I5H000 Backend link error was detected(Unit-06,ENC-0) W0FA00 ENC alarm(Unit-06,ENC-0) :ENC /STR" [Conditions of Occurrence] The problem occurs when all following conditions are met. 1. Partial retry occurs in Discover. 2. The result of the retry is GOOD or Reject. 3. Linkup of ENC is slow. [Cause] Due to the firmware bug about SAS management.	
	V6.0, 0860/C							1/29/2009　91
V6.0, 0860/C Base System V6.0/B, 0860/B	1	C	B	D800-53278, EUC 922630	V60-0286	When a TC pair size was 8 TB, remote paths were blockaded, and then the pair status became PSUE.	[Phenomena] When a TC pair size was 8 TB, remote paths were blockaded, and then the pair status became PSUE. [Conditions of Occurrence] If the following conditions are met, PSUE or Auto Migration failure occurs. A. TrueCopy remote replication or TrueCopy Extended Distance or Simple Data Recovery or AutoMigration is used. TrueCopy remote replication /TrueCopy Extended Distance (supported by DF800 only) Simple Data Recovery (supported by SA800/SA810 only) AutoMigration (Only online array replacement) (supported by SA800/SA810 only) B. A Pair is created or The Auto Migration (selected online array replacement) is executed for a LU, which size is over 8 TB (including LUN expansion). [Cause] Firmware bug. A Check process of the vendor unique command using a remote replication function of DF800/SA800/SA810 had a bug. The check process targets 2nd bit (bit value is 0x04) of 16th byte of the command. However the process targeted the 6th byte wrongly. As a result, in case of a TC pair size is over 8 TB, remote paths become failure when total data transfer size becomes	
	V6.2, 0862/A							2/25/2009　100
V6.2, 0862/A Base System V6.0/C	1	N	-		None	TrueCopy Modular Distributed	TrueCopy Modular Distributed (Fan-In/Fan-Out) is supported.	
	2	N	-		None	SI Quick Resync/Split	Quick Resync/Split for ShadowImage in-system replication is supported.	
	3	N	-		None	IPv6 for LAN(SNMP)	IPv6 for LAN(SNMP) is supported.	

V8.0/C, 0860/C	4	C	C		V62-0001	A session from SNM may encounter invalid timeout while using account authetication	[Phenomena] A user may not be able to log on to an array from SNM due to invalid timeout while using account authetication even if the specified timeout has not been reached. Or, a user may stay logged on from SNM while using account authentication even if the specified timeout has been reached. [Conditions of Occurrence] < Equipment model > DF800H/M/S (SA800/SA810) < Firmware version > DF800: 0832/A and later (SA800/SA810: 1832/A and later) <Related Program Product> Account Authentication <Conditions of occurrence> If the following conditions are met, invalid time may occurs. A. Account Authentication is enabled B. CTC timer in the master CTL and the slave CTL are not synchronized C. An access from SNM is tried but it reached a slave CTL that is different from the one previously accessed due to failure on network or CTL. [Cause] Firmware bug. Timeout check is done on the master CTL. If the CTC timer in the master CTL and the slave CTL are not synchronized, if a session
	5	C	B		V62-0034	CTL recovery failure when on-line CTL replacing is executed after CTL failure by "Backend link error".	[Phenomena] CTL recovery failure when on-line CTL replacing is executed after CTL failure by "Backend link error". [Conditions of Occurrence] <Equipment model> DF800H <Firmware version> 0850/A or later <Conditions of Occurrence> The problem occurs when all following conditions are met. 1. There are less than 29 RKAs connected. 2. CTL failure occur because of Backend link failure of ENC in CTL unit. 3. Executing on-line CTL replacing. [Cause] Due to firmware bug about ENC blockade proccessing and CTL recovery proccessing.
	6	C	C		V62-0065	When SnapShot changed to PSUE, SNMP Trap is issued by mistake.	[Phenomena] When SnapShot changed to PSUE, SNMP Trap of Snapshot is issued. And SNMP Trap of ShadowImage is issued by mistake. [Conditions of Occurrence] If the following conditions are met, invalid time may occurs. A. SNMP Trap is enabled B. SnapShot changed to PSUE [Cause] Due to the firmware bug about SNMP
	7	C	B		V62-S009	CTL cannot excute I/Os to SATA HDD when the HDD failure occurs during ENC firmware download.	[Phenomena] CTL cannot excute I/Os to SATA HDD when the HDD failure occurs during ENC firmware download. [Conditions of Occurrence] <Equipment model> DF800H/M/S, SA800 <Firmware version> DF800 0832/A or later, SA800 1811/A-B or later <Conditions of Occurrence> The problem occurs when all following conditions are met. 1. There are SATA HDDs in system. 2. ENC firmware download is executed. 3. SATA HDD failure occure. [Cause] Due to the firmware bug about SATA HDD failure proccessing
	8	C	B		V62-B002	Controller is blockaded with "Microprogram error[BER]" when TrueCopy pair status changes during ENC firmware download process.	[Phenomena] Controller is blockaded with "Microprogram error[BER]" when TrueCopy pair status changes during ENC firmware download process. The message "Microprogram error[BER]" is displayed. [Conditions of Occurrence] The problem may occur when all following conditions are met. 1.TrueCopy is available 2.TrueCopy pair status change is operated. 3. During #2 is executed, ENC firmware download is processing or backend failure occurs at the TrueCopy remote site. [Cause] Due to the firmware bug about backend recovery process when TrueCopy pair status changes
	9	C	B		V62-0073	Multiple HDDs are blockaded when a controller is blockaded.	[Phenomena] When a controller is blockaded, multiple HDDs are blockaded with HDD timeout or OPEN_FAILURE_RETRY. [Conditions of Occurrence] The problem may occur when all following conditions are met. 1. Special process (due to exclusive status between both controllers) is executed. 2. Capturing process of PHY ERROR LOG in the backend root is executed because HDD path failure occurs. 3. Failure occurs. The recovery process of the failure includes SAS chip reset. 4. Failure occurs with SAS HDD reset after #3. The recovery process of the failure includes SAS chip reset. [Cause] Due to the firmware bug about backend recovery process after SAS HDD reset.

	10	C	B		V62-0076	CTL cannot excute I/Os because of issuing multiple reset commands to SATA HDD	[Phenomena] I/O stop because of issuing multiple reset commands to SATA HDD. When timeout occurs on both ports of SATA HDD during LinkDown failure of backend, multiple reset comands are issued. As a result, issuing reset commands continues and special process(due to exclusive status between both controllers) doesn't finish. [Conditions of Occurrence] The problem may occur when all following conditions are met. 1. Special process (due to exclusive status between both controllers) is executed. 2. LinkDown failure of backend occurs and LinkUp diagnostic is executed. 3. During #2 is executed (about 1 second), timeout occurs on both ports of SATA HDD [Cause] Due to the firmware bug about backend recovery process after
	11	C	B		DCPS-006	When a CTL fails, the ports on opposite CTL cannot Link up.	[Phenomena] When a CTL is in the failure or CHK1, the ports on opposite CTL, that status is Ready, cannot Link up. [Conditions of Occurrence] < Equipment model > DF800H < Firmware version > DF800: 0843/B or later <Conditions of occurrence> If all the following conditions are met, the phenomenon occurs.. 1. FC I/F is implemented 2. Link down occurs on an FC Port. 3. The "Transfer Rate Setting" of the Port that is mentioned at #2 specified to "Auto" (default). 4. In case the opposite CTL of the port exists is in the status of Failure or CHK1 right after the Link down mention at #2 occurs. [Cause]
	12	C	B		V61QP010	A CTL fails after the double HDU failure	[Phenomena] When the huge amount (more than 11278) of PIN data exits, a CTL failure caused by LU failure occurs with HDU failure. [Conditions of Occurrence] < Equipment model > DF800H/M/S (SA800/SA810) < Firmware version > DF800: 0832/A or later (SA800/SA810: 1810/N and later) <Conditions of occurrence> If all the following conditions are met, the phenomenon occurs.. 1. One CTL or Core have huge amount of PIN data. 2. Drive Detach mode is enabled 3. LU failure occurs because that HDU fail and the RG have no redundancy [Cause] Firmware bug related to the process to delete the PIN data when the LU failure occurs.
	13	C	B		V62-B005	I/O error or CTL failure may occur during firmv	[Phenomena] I/O error or CTL failure may occur during firmware update. [Conditions of Occurrence] < Equipment model > DF800H/M/S FC I/F only SA800/SA810 FC I/F only < Firmware version > DF800: 0832/B and later SA800/SA810: 1832/C and later <Related Program Product> None <Conditions of occurrence> I/O error may occur during online firmware update. If link error occurs after the I/O error during online firmware update, CTL failure will occur at the timing of automatic or manual recovery. [Cause] Firmware bug. The flag that shows the status of firmware update process

V6.0, 0860/C Base System V6.0/B, 0860/B	1	C	B	D800-53278, EUC 922630	V60-0286	When a TC pair size was 8 TB, remote paths were blockaded, and then the pair status became PSUE.	[Phenomena] When a TC pair size was 8 TB, remote paths were blockaded, and then the pair status became PSUE. [Conditions of Occurrence] If the following conditions are met, PSUE or Auto Migration failure occurs. A. TrueCopy remote replication or TrueCopy Extended Distance or Simple Data Recovery or AutoMigration is used. TrueCopy remote replication /TrueCopy Extended Distance (supported by DF800 only) Simple Data Recovery (supported by SA800/SA810 only) AutoMigration (Only online array replacement) (supported by SA800/SA810 only) B. A Pair is created or The Auto Migration (selected online array replacement) is executed for a LU, which size is over 8 TB (including LUN expansion). [Cause] Firmware bug. A Check process of the vendor unique command using a remote replication function of DF800/SA800/SA810 had a bug. The check process targets 2nd bit (bit value is 0x04) of 16th byte of the command. However the process targeted the 6th byte wrongly. As a result, in case of a TC pair size is over 8 TB, remote paths become failure when total data transfer size becomes over 8TB			
	V6.5, 0865/B							5/11/2009	103Rev3	009
V6.5, 0865/B Base System V6.2/A, 0862/A	1	I	A		None	Quality improvement of back end error processing.	1) Execution time check logic for the drive access has been improved. The back end blockage due to the time-out error will reduce by this improvement 2) Improvement of the time-out value in the back end diagnosis and the drive blockage condition.			
	2	I	A		None	The host IO stop time has been shortened on controller reboot and non stop online microcode update.	1) The processing time of initialization including the cache memory executed by processing the controller rebooting and the non stop microcode update has been shortened.			
	3	C	B	D800-53343	V65-0079	Countermeasure against random IO performance degradation	There is a probability that random I/O performance downs when both random I/O and sequential I/O are executed in the same system. < Equipment model > DF800H/M/S < Firmware version > DF800: 0850/D and later			
	4	C	C		V65-QP002	Countermeasure of Online Forced Parity Collection	The Online Forced Parity Collection is not completed from the "Waiting" state. <Equipment model> DF800H/M/S,SA800/SA810 <Firmware version> DF800 First version or later SA8x0 First version or later <Conditions of Occurrence> When the Online Forced Parity Collection instruction from SNM and the Mode select command from host compete.			
	5	C	B		V65-B001	Countermeasure against CTL blockage after when a Program Products is installed	Countermeasure against CTL blockage after when a Program Products is installed "CACHERESIDENCY"."SNMP-GENT"."SHADOWIMAGE"."LUN-MANAGER"."SNAPSHOT"."PFM-MONITOR"."AUDIT-OGGING" The blockage factor message at this time is "Resource release time-out". <Equipment model> DF800H/M/S,SA800/SA810 <Firmware version> DF800 First version or later SA8x0 First version or later <Conditions of Occurrence>			
	6	C	C		V65-0004	Countermeasure against path alarm at the login request from another processor core.	When TC or TCE is used, the host command time-out and the Path alarm are occurred. <Equipment model> DF800H/M/S,SA800/SA810 <Firmware version> DF800 First version or later SA8x0 First version or later <Conditions of Occurrence> The problem occurs when all following conditions are met. 1.TC or TCE use 2.State of login 3 The login request (PLOGI transmission request) was			
	7	C	B		V65-0084	Countermeasure against CTL blockage by consecutive uncorrectable error.	When the uncorrectable error is detected by the verify retrying processing, then CTL is blockaded by "Microprogramerror RCH". <Equipment model> DF800H/M/S,SA800/SA810 <Firmware version> DF800 First version or later SA8x0 First version or later <Conditions of Occurrence> The problem occurs when all following conditions are met. 1. SAS HDD. 2. A RAID group has no Redundancy . 3. Media error was occurred by the collective write. 4. Media error was occurred by the retrying (as reassign, write			

	8	C	C		V65-QA024	Countermeasure against CTL blockage when CPM is used	When SS or TCED was enabled, CTL might be blockaded. The CTL obstructive cause is the following. Host transfer DMA error" Parity generation LA error " <Equipment model> DF800H/M/S,SA800/SA810 <Firmware version> DF800 First version or later SA8x0 First version or later <Conditions of Occurrence> The problem occurs when all following conditions are met. 1. SS/TCED is invalid. 2. CPM is enable. 3. The LU unit is being switch ed. 4. SS or TCED is enable.
	9	C	C		V65-QP009	Countermeasure against CTL blockage by HSNM2 operation.	When LU is deleted from HSNM2 during I/O execution , the CTL is blockaded by "Microprogram error FSM". <Equipment model> DF800H/M/S,SA800/SA810 <Firmware version> DF800 First version or later SA8x0 First version or later <Conditions of Occurrence> The problem occurs when all following conditions are met. 1. Host I/O is being processed. 2. A setting or reference through HSNM2 GUI or CLI is operated. 3. The host command processing competed with the
	10	C	B		V65-QA028	Countermeasure against CTL blockage by the false detection of hardware failure when the host I/O load is high.	When LU is remove during host I/O operation, CTL is blockaded with message "H06J00 [DCTL]The unexpected completion was detected[E_IRQ6](CTL-0)". <Equipment model> DF800H <Conditions of Occurrence> The problem occurs when all following conditions are met. - FC host I/F - Two FC I/C boards are installed to both CTL and more then 4 ports are used on the both of CTL . - Host I/O load is high.
	11	C	B		V65-0098	Countermeasure against CTL blockage caused by iSCSI login/logout during non-disruptive firmware update	CTL is blockaded accidentally by execution of iSCSI login/logout during non-disruptive firmware update. Following message is issued: [Web Message]"H0D001 Synchronization failure of the MPU core was detected[INM](CTL-1) :CTL /FDM" <Conditions of Occurrence> The problem occurs when all following conditions are met. (1) DF800H with iSCSI I/F (2) non-disruptive firmware update. (3) iSCSI login or logout is received from a host.
	12	C	A		V65-QA030	Countermeasure against the impossibility for processing I/Os when a failure occurs during non-disruptive firmware update	On a subsystem with TC configuration where I/Os are executed, non-disruptive firmware update is executed. Then I/Os are not executed by the subsystem, though the subsystem is ready. <Conditions of Occurrence> The problem occurs when all following conditions are met. (1) TC with iSCSI host I/F (2) Write I/O to the pair of TC, where the status of the pair is PAIR or COPY. (3) During Initiator data transfer, timeout (27sec) occurs by the path failure or by the failure of remote subsystem.
	13	C	A	D800-53415	V65-0112	Countermeasure against blockage of ENCs When installing CTL with cable connection mistakes	On DF800M(Basic Tray + several Additional Trays), when replacing a CTL, its ENC cable of Path 0 and Path 1 was connected inversely. The CTL is inserted, then Unit1-ENC0 is blockaded with message "ENC recovery failed[Cable error]" and ENC alarm occurred at Unit1-ENC1. Thus both of ENCs in Unit1 is blockaded and the subsystem is down with the message: "Backend has been down[All the routes have been blockaded]". <Equipment model> DF800H or DF800M or DF800S <Conditions of Occurrence> (1) CTL is blockaded. (2) The CTL is replaced.
	14	C	B		V65-0100	Countermeasure against impossibility of recover from ACA state	If CTL blockage occurs just after the CHECK response to the host command, recovery from ACA status is not done even receiving Clear ACA. (i.e. the CTL cannot execute host I/Os) <Equipment model> DF800H or DF800M or DF800S <Conditions of Occurrence> The problem occurs when all following conditions are met. (1) NACA mode is enable as the host group option. (AIX host connection) (2) A command is revived through the CTL cross-call. (3) The response to the command of (2) is CHECK and the device become ACA state (Auto Contingent Allegiance. I/Os cannot be operated until Clear ACA command is received.) (4) During the state change of (3) (min 2 micro seconds to max

	15	C	B		V65-0117 (V70QP001)	Countermeasure against wrong check of LUN range when changing a pair name	(1) Creating TC pair between DF800S(PVOL) and DF800H (LUN1-LUN2505) (2) Changing the pair name of the TC pair from DF800S, but the operation failed with the error message: "DMEDC00002: The process cannot be performed because the specified logical unit number is outside the effective range. Please confirm the logical number." <Conditions of Occurrence> The problem occurs when all following conditions are met. <Equipment model> Local subsystem: DF800S Remote subsystem: DF800M/DF800H/DF700H or Local subsystem: DF800M/DF800H/DF700H Remote subsystem: DF800S <Environment> - HSNM2 for operations - TC/TCE is used <Operations> - Change the name of the pair which is already created. (The max number of LUs of the subsystem is less than or equal
	16	C	B	D800-23457	V65-0027	Countermeasure against wrong blockage of ENC during format	Unit0-ENC0 is blockaded falsely during LU format. Command timeouts of backend commands from Y core to X core caused this blockage as the threshold over of command timeout. <Conditions of Occurrence> The problem occurs when all following conditions are met. <Equipment model> DF800H <Operation> (1) Both CTL are Ready state. (2) Both CTL issue write commands of long data (256KB or longer data length) (3) The target HDU of the commands of (2) is more than 6.
	17	C	B	SA800-23461	V65-0121	Countermeasure against access lost of iSCSI connection from host	Access lost of iSCSI connection from host occurred. <Equipment model> DF800H/M/S,SA800/SA810 <Conditions of Occurrence> The problem occurs when all following conditions are met. (1) iSCSI I/F (2) Receiving a command which is to be processed cross-call between CTL from host. (e.g. A command to the LU whose ownership is not belong to the CTL which received the command.)
	18	C	C		-	Update of HDD Firmware	There is a case where an HDD (Hard Disk Drive) access may become timeout falsely. <Equipment model> DF800H/M/S <Conditions of Occurrence> The problem occurs when all following conditions are met. (1) HDD: AKF400(S), AKH146(S), AKH300(S), AKH146(S1), AKH300(S1), AKH450(S) (2) ENC is blockaded during host I/O processing. <Cause> HDD Firmware bug. A drive doesn't complete Abort Command processing in some case. Then the firmware (microprogram) recognize that drive I/O as timeout. [Countermeasure] Update the HDD firmware, where they are included in the firmware (microprogram): AKF400(S) : 4C04 --> 4C07 AKH146(S) : 4C58 --> 4C5B AKH300(S) : 4C58 --> 4C5B AKH146(S1) : 4C54 --> 4C55 AKH300(S1) : 4C54 --> 4C55 AKH450(S) : 4C54 --> 4C55
	19	C	C		V65-0021	Countermeasure against illegal indication of iSCSI FW version on TDCONV after non-disruptive firmware update	TDCONV indicates different iSCSI FW version between controller0 and controller1 after non-disruptive firmware update. <Equipment model> DF800H/M/S <Conditions of Occurrence> The problem occurs when all following conditions are met. (1)iSCSI I/F (2)non-disruptive firmware update between firmware versions that have different iSCSI FW version (3)iSCSI FW version is indicated by TDCONV. <Cause> Firmware bug. Because ready controller updates iSCSI FW version on reboot controller, old iSCSI FW version is illegally written in indication information area on reboot controller.

	20	C	B		V65-0046	Countermeasure against the impossibility for processing during non-disruptive firmware update	When non-disruptive firmware update is executed, cross call I/Os are not executed by the subsystem from reboot start to ready status of reboot controller. <Equipment model> DF800H <Conditions of Occurrence> The problem may occur when all following conditions are met. (1) DF800H (2) Cross call I/Os are executed during non-disruptive firmware update <Cause> Firmware bug. Because the reboot controller of DF800H illegally has a control authority about FrontEnd protocol chip during reboot timing, the ready controller cannot execute cross call I/Os.		
	V6.5, 0865/D							5/29/2009	118	011
V6.5, 0865/D Base System V6.5/B, 0865/B	1	C	A	D800-53482 EUC990092	V65-0123	Countermeasure against subsystem outage that occurs when a LU that has equal or more than 256 HDDs is created.	Subsystem outage occurs when a LU in a RAID group consisted of equal or more than 256 HDDs is created and the LU is formatted. H90320 Watch-dog time-out or HZ0N01 Kernel processing error(CTL-1) HZ0N00 Kernel processing error(CTL-0) < Equipment model > DF800H < Firmware version > DF800: 0840/A and later <Conditions of occurrence> The problem occurs when all following conditions are met. - A LU in a RAID group consisted of equal or more than 256 HDDs is created. - The LU is formatted.		
	2	C	A		V65-0124	Countermeasure against subsystem outage by the false detection of hardware failure when the host I/O load is high.	During host I/O operation, subsystem outage occurs with message "The internal parity error of the configuration read was detected[E_IRQ6]" for the both controllers. <Equipment model> DF800H <Firmware version> DF800 First version or later <Conditions of Occurrence> The problem may occur when all following conditions are met. - DF800H - FC host I/F - 2 FC I/C boards are installed to each controller and more than 4 ports are used on the each controller . - Host I/O load is high.		
	3	C	A	D800-23624 EUC998394	V65-0125	Countermeasure against subsystem outage that occurs when V-Vol of Snapshot is read in PSUS status.	Subsystem outage occurs when V-Vol of Snapshot is read in PSUS status. HJ11OV Microprogram error [RCH] H90210 CTL failure W01200 CTL alarm (CTL-0) <Equipment model> DF800H/M/S <Firmware version> DF800 0852/A or later <Conditions of Occurrence> The problem occurs when all following conditions are met. - Firmware version V5.2/A or later - Snapshot is used. - P-Vol and Pool-Vol of Snapshot belong to RAID group below each other. P-Vol=RAID1, Pool-Vol=RAID5, or P-Vol=RAID1, Pool-Vol=RAID6, or P-Vol=RAID0+1, Pool-Vol=RAID5, or P-Vol=RAID0+1, Pool-Vol=RAID6, or P-Vol=RAID5, Pool-Vol=RAID1, or P-Vol=RAID5, Pool-Vol=RAID0+1, or P-Vol=RAID6, Pool-Vol=RAID1, or P-Vol=RAID6, Pool-Vol=RAID0+1 - The Snapshot pair is in PSUS status - New data is written in P-Vol area. Then V-Vol area related to the P-Vol area is read.		
	4	C	B		V70-0512 (V65-0126)	Countermeasure against SATA HDDs blockade during subsystem booting without one controller.	During subsystem booting without one controller, "HDU spin up failed" occurs and SATA HDDs are blockaded. <Equipment model> DF800H/M/S <Firmware version> DF800 First version or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (1) When SATA HDDs are spined up in case of the conditions below and then broadcast notification that indicates "SATA HDD Link Up" is notified to the controller during backend discover process, the problem may occur. - SATA HDDs spin up except system HDDs during subsystem booting - SATA HDDs spin up when additional units are added		

	5	C	A		V70-0510 (V65-0127)	Countermeasure against subsystem outage that occurs when Soft Reset for iSCSI chip is executed in case that the failure occurs during host I/O.	When Soft Reset for iSCSI chip is executed in case that the failure occurs during host I/O, the both controllers are blockaded with Microprogram error[ISM] and subsystem outage occurs. HH7Dxy Microprogram error[ISM] <Equipment model> DF800H/M/S <Firmware version> DF800 First version or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (1) iSCSI I/F (2) Cross call access is executed between the both controllers (3) Failure occurs. The failure should be recovered by Soft Reset for iSCSI Chip (No response for data transfer request) (4) When only one request to execute the command is set on the controller, Soft Reset for iSCSI chip occurs.			
	6	C	B		IHV-0019	Countermeasure against unrecoverable host path status after firmware exchange with reboot.	When firmware exchange with reboot is executed on iSCSI configuratio, host path status is unrecoverble after firmware exchange. <Equipment model> DF800H/M/S <Firmware version> DF800 First version or later <Conditions of Occurrence> The problem occurs when all following conditions are met. (1) iSCSI I/F (2) firmware exchange with reboot is executed (3) The controller receives host command in five seconds before controller READY status after reboot. And then the host doesn't retry the command.			
	7	C	B		V70-QA001 (V65-0128)	Countermeasure against controller blockade when Resource release time-out is detected in case that cache uncorrectable error occurs.	In case that cache uncorrectable error occurs, maintenance change parts is cache. But when Resource release time-out (similar to hung-up) is detected, maintenance change parts is the controller illegally. According to maintenance change message, if controller is changed and cache is not changed, this phenomena may occur again. <Equipment model> DF800H/M/S <Firmware version> DF800 First version or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (1) DF800H (2) FC I/F (3) Controller is blockaded because of cache uncorrectable error			
	8	C	A		V70-0423 (V65-0129)	Countermeasure against subsystem outage with message "Data transfer check error[CCPLUNERR]" when "paircreate -split" command of ShadowImage is executed.	<Equipment model> DF800H/M/S <Firmware version> DF800 First version or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (1) ShadowImage is used. (2) One or more pair of ShadowImage that belongs "CTG (consistency group)" exist. (3) Host I/Os are executed to a ShadowImage pair below. In case of DF800H/M/S, the pair belongs to the different controller from the controller to which a pair (copy status) belongs. In case of DF800M/S, the pair belongs to the different CPU core on the same controller from the CPU core to which a pair (copy status) belongs. (4) Pair operation command is executed below. pari create and split command (paircreate –split) or suspend comannd (includes "for quick mode") during paircreation or suspend comannd with quick mode during pair-resync or suspend comannd during pair-resync with quick mode			
	V7.0, 0870/C							6/5/2009	121	None
V7.0, 0870/C Base System V6.5/D, 0865/D	1	N	-			Hitachi Dynamic Provisioning	Hitachi Dynamic Provisioning is supported.			
	2	N	-			DC power supply	Air filters replacement alert for DC power supply is supported.			
	3	N	-			Additional battery	Additional battery for DC power supply is supported.			
	4	I	-			Account Authentication	The usability of HSNM2 GUI for Account Authentication is improved.			
	5	I	-			The firmware of iSCSI chip	The firmware version of iSCSI chip is upgraded. (Rev.58)			
	6	C	B		V70-0474	Countermeasure against host linkup failure occurs when executing firmware update in online.	The host linkup failure occurs when FC link failure occures during executing firmware update in online. < Equipment model > DF800 < Firmware version > DF800: First version or later <Conditions of occurrence> The problem may occur when all following conditions are met. - The firmware update is executed. - The FC link failure occurs.			

	7	C	C		V70-V4.0.0	Including the network patch of the internal OS.	The new firmware includes the network patch for the vulnerability strengthening of the Web, DHCP and TCP protocol. <Equipment model> DF800 SA800/SA810 <Firmware version> DF800: First version or later SA800/SA810: First version or later <Conditions of Occurrence> The problem may occur when LAN is connecting to the controllers.
	8	C	B		V70-0045 V70-0529	Countermeasure against HDD blockade occurs when the backend failure occurs.	One or more HDDs are blockaded incorrectly when the backend failure occurs. (But this issue was discovered by source code check and has NOT occurred at machine.) <Equipment model> DF800 <Firmware version> DF800: First version or later <Conditions of Occurrence> The problem occurs when all following conditions are met. - The subsystem is booting or stopping. - The path failure of backend occurs.
	9	C	B		V70-0116 V70-0030 V70-0289 V70-0496 V70-0457 V70-0504 V70-0516 V70-0538	Countermeasure against ENC or controller blockade occurs when the backend diagnosis is executed.	The ENC or controller blockade occurs when the backend diagnosis is executed for some hardware failure during downloading the ENC firmware, exchanging the ENC or subsystem is booting. <Equipment model> DF800 <Firmware version> DF800: First version or later <Conditions of Occurrence> The problem may occur when all following conditions are met. - The backend diagnosis is executed during the ENC firmware is downloading, inserting ENC or - The backend diagnosis is executed during inserting HDD. or - The backend diagnosis is executed during subsystem is booting.
	10	C	B		V70-0043	Countermeasure against account authentication responds incorrectly for Mode Sense and LAN Sense command.	When Mode Sence/LAN Sence is issued with the account authentication log in bit ON, a response that is issued in page 3E_55H is defferent from a response that is issued in other pages. (This problem is discovered at Hi-Track evaluation.) <Equipment model> DF800 SA800/SA810 <Firmware version> DF800: First version or later SA800/SA810: First version or later <Conditions of Occurrence> The problem may occur when all following conditions are met. - When a Host issues Mode Sense/LAN Sence. - When an account authentication bit is ON.
	11	C	B		V70-0332	Countermeasure against the host timeout that occurs on the host connected to another side of controller when the controller blockades.	The host detects a timeout error when LU ownership change and controller blockade occur in same time. <Equipment model> DF800 <Firmware version> DF800: First version or later <Conditions of Occurrence> The problem may occur when all following conditions are met. - LU ownership change occurs during the host issues read command. - The read data does not exist in cache memory. - The controller that is new owner of LU blockades during transferring the read data.
	12	C	B		V70-0392	Countermeasure against the controller blockade occurs when the Verify command is received.	The controller blockade ocuurs with the message "Microprogram error[SCK]" when the verify command is issued to the subsystem that "Verify Skip Mode" is set to OFF and backend failure occurs in same time. <Equipment model> DF800 SA800/SA810 <Firmware version> DF800: First version or later SA800/SA810: First version or later <Conditions of Occurrence> The problem may occur when all following conditions are met. - The parameter "Verify Skip Mode" is set to OFF. - The verify command is issued from host. - The backend failure occurs.

	13	C	B		V70-0469	Countermeasure against the ShadowImage pair becomes PSUE status when the host issues write command to P-VOL or S-VOL that is in PSUS(SP) status.	The pair of ShadowImage becomes PSUE status when the host issues write command to the P-VOL or S-VOL that is in PSUS(SP) status. <Equipment model> DF800 SA800/SA810 <Firmware version> DF800: 0862/A or later SA800/SA810: 1862/A or later <Conditions of Occurrence> The problem may occur when all following conditions are met. - The pair is constituted from LUs that is 10GB or more. - The host issues write command to the P-VOL or S-VOL that is in PSUS(SP) status. - The position where the data copy interruption position and the write command are accepted is within 10GB.			
	14	C	C		V70-0362	Countermeasure against the outputting full dump does not work correctly.	The outputting full dump does not work correctly after the full dump is outputted once. <Equipment model> DF800 <Firmware version> DF800: 0860/A or later <Conditions of Occurrence> The problem may occur when all following conditions are met. The problem occurs when all following conditions are met. - The full dump is outputted twice. (This phenomena does not occurred when subsystem is re-booted or soft reset swtich is used.)			
	15	C	B		V70-BP16	Countermeasure against the I/O error occurs in host side when the controller recovers from the failure.	The I/O error occurs in host side when the controller recovers from the failure. (If the application retry the command, good will be returned to host.) <Equipment model> DF800 <Firmware version> DF800: First version or later <Conditions of Occurrence> The problem may occur when all following conditions are met. - FC I/F is installed on subsystem. - The controller is recovering from the failure. - The host issues I/O to the other controller.			
	16	C	B		V70-0510	Countermeasure against the controller blockade occurs when iSCSI chip failure occurs.	The controller blockade occurs with the message "Microprogram error[ISM]" when iSCSI chip failure that is recoverable occurs during host I/O is receiving. <Equipment model> DF800 SA800/SA810 <Firmware version> DF800: First version or later SA800/SA810: First version or later <Conditions of Occurrence> The problem may occur when all following conditions are met. - The iSCSI I/F is installed on subsystem. - The host issues I/O to the subsystem. - The iSCSI chip failure occurs that is recoverable.			
	17	C	B		V70QP004	Countermeasure against the incorrect message is displayed when the TrueCopy is used.	The incorrect message is displayed when the operation for the TrueCopy pair is executed during the firmware update is executed in online. (The error should be displayed if the operation for the TrueCopy pair is executed during the firmware update, but message is not correct.) DMEA00000A The CHECK CONDITION status was reported from the subsystem, but the details could not be acquired. Please retry after waiting for a while. <Equipment model> DF800 <Firmware version> DF800: First version or later <Conditions of Occurrence> The problem may occur when all following conditions are met. - The firmware update is executed in online. - The operation for the TrueCopy pair is executed.			
	18	C	B		V70-0520	Countermeasure against controller blockade occurs when the forced parity recovery is executing during expanding RG.	The controller blockade occurs when the forced parity recovery is executing due to recovery from cache volatilizing after accidentally stopping of power supply during expanding RG. <Equipment model> DF800 SA800/SA810 <Firmware version> DF800: First version or later SA800/SA810: First version or later <Conditions of Occurrence> The problem may occur when all following conditions are met. - The stopping power supply occurs accidentally during expanding RG. - On the same stripe row in the range of parity recover, there exist uncompleted write date and LA/LRC error.			
	V7.2, 0872/A							6/30/2009	130	None

V7.2, 0872/A Base System V7.0/C, 0870/C	1	N	-	-	None	SH543; 8Gbps FC I/F Board support	Firmware bug. Because the overhead increses for cache segment lock process between dual cores. <Details> (a) The free segments is shared by Xcore and Ycore. So, the firmware processes the exclusion when the free segments are used or discharged.	
	2	N	-	-	None	RADIUS (for Account Authentication)	RADIUS (for Account Authentication) is supported.	
	3	N	-	DF700-53163 DF700-22446 (SD2494549) D700-80896 (SD2512286) D700-22491 (SD2504869) DF700-22401 (SD2490065) D700-22236 (SD2467616)	DF700-0251	Online Cache Verification Function	New microcode automatically executes the online preventive diagnosis in addition to existing power-on diagnosis for the cache memories.	
	4	I	-	-	None	Enhancement of Dynamic Provisioning (DMLU, CMDDEV)	DP volume is supported to be assigned to DMLU or CMDDEV.	
	5	I	-	-	None	Guard against single mode when Dynamic Provisioning is enabled	Guard against single mode, when HDP is enabled, is supported.	
	6	I	-	-	V72-0073	Check whether DP volume creation/expansion is possible or not	Check whether DP volume creation/expansion is possible or not is supported.	
	7	I	-	-	None	Improvement of the usability of HSNM2 GUI on the setting of port security	Improvement of the usability of HSNM2 GUI on the setting of port security	
	8	C	A	DF700-23044	V72-0009 (DF700V82-0016)	Countermeasure against the booting failure when all the system-disk areas are unavailable.	Booting failure when all the system-disk areas are unavailable. <Equipment model> DF800H/M/S <Firmware version> First version or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (1) Subsystem boot up (2) All the system-disk areas (i.e. system areas for DF in the first 5 HDDS) are not available because of HDD failures etc.	
	9	C	A	DF700-53166, DF700-53272(EUC937860)	V72-0022	Countermeasure against LA/LRC errors during forced parity rebuild	In both CTLs, Cache ECC uncorrectable error occurs. So, the subsystem is outage and the user date has lost. Then LA/LRC errors are detected in the plural HDDs during forced parity rebuild. (Thus the rebuild failed). The correction copy of the failed HDD were also failed by LR/LRC errors in the other HDD in the same RAID Group. <Equipment model> DF800H/M/S <Firmware version> First version or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (1) No redundancy of CTL (i.e. Single CTL or Dual CTL with one CTL blockaded) (2) ECC uncorrectable Error of cache memory is detected	
	10	C	A	D800-53415 (EUC971559)	V72-0026	Countermeasure against subsystem outage caused by a wrong connection of ENC cable in online controller exchange.	When Controller is exchanged with wrong connection of ENC cable, subsystem outage occurred with following Web messages: HH8W00 Backend has been down[All the routes have been blockaded] W0FA00 ENC alarm(Unit-01,ENC-1) I5HB00 ENC recovery failed[Cable error](Unit-01,ENC-0) W0FA00 ENC alarm(Unit-01,ENC-0) I1G300 CTL recovery start(CTL-X) <Equipment model> DF800H/M/S <Firmware version> V3.0 (Rev. 0830/A) or later <Conditions of Occurrence> The failure occurs when the followings conditions are met. -Subsystem configuration has 2 RKAK/RKAKX or more. -Online controller exchange is executed with wrong connection of	
	11	C	A	-	V72QA009	Countermeasure against data inconsistency on DP-Vol deletion or DP-Vol format after PS OFF/ON	When the PS OFF/ON is executed after the DP-Vol deletion or DP-Vol formatting, the data inconsistency may occur. <Equipment model> DF800H/M/S <Firmware version> V7.0/C (Rev. 0870/C) <Conditions of Occurrence> The failure may occur when the followings conditions are met. - Firmware version V7.0/C - DF800H/M/S - Using the Dynamic Provisioning function - Executing the DP-Vol deletion or DP-Vol formatting - The PS OFF/ON is executed after the above operatons. - The size of DP-RG in the DP pool is more than 1TB	
	12	C	B	-	V72-S006	Countermeasure against CTL blockade due to the loading failure of iSCSI firmware during PS OFF/ON heat run	CTL was blockaded on planned shutdown. The planned shutdown itself was completed. <Equipment model> DF800H/M/S <Firmware version> First version or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (1) iSCSI I/F (2) Due to IP address change or some failure on iSCSI, reset to iSCSI protocol chip is done. (3) Planned shutdown is done during the recovery process from the reset of (2).	

	13	C	B	-	V72QA020	Countermeasure against error responses for I/Os after the CTL blockade and the recovery	Error responses (04/4400 hardware error) are issued for I/Os after the CTL blockade and the recovery . - If connected to host, and if a failover software is used, the I/O will be processed on the other CTL after the failover. - If connected to DF or SA (by copy function), the pair will become PSUE or the path will be blockaded. - If connected to RAID (by UVM), the path will be blockaded. In case of firmware update (either nonstop or path failover) instead of CTL blockade, this issue doesnot occur. <Equipment model> DF800H/M/S <Firmware version> 0850/A or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (a) Configurations (1) Firmware: 1850/A or later (2) DF800H/M/S, SA8x0 (3) Connected to higher-level devices (hosts, DF or SA for copy: TC/TCE/SimpleDR, RAID for UVM) through Fibre Channel interface (b) Conditions (1) Plural write I/Os from higher-level devices are processed by Active-Active (cross-call among CTLs). (2) Then the CTL where receiving write I/Os is blockaded. (3) Then the CTL of (2) recovers.
	14	C	C	DF700-53391	V72-0014 (DF700V82-0014)	Countermeasure against the access loss on rebooting AIX server connected through FC port.	Access from hosts (connected through an FC port of the subsystem) are lost when an AIX server (connected through the same port) is rebooted. <Equipment model> DF800H/M/S <Firmware version> First version or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (1) An AIX server is connected to an FC port of the subsystem. (2) Other hosts are accessing through the same port. (3) Rebooting the AIX server. (Then the AIX server issues the Request Sense command with FCP_DL=0 and CDB length =
	15	C	C	-	V72-0051	Countermeasure against incorrect message on the failure of account authentication on the reboot request of a subsystem	Incorrect message (DMED001F00) on the failure of account authentication on the reboot request of a subsystem is issued. <Equipment model> DF800H/M/S <Firmware version> First version or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (1)AMS2100/2300/2500 (2) Account Authentication P.P. is enabled (3) Reboot request from HSNM2 (4) Failure of account authentication due to the followings: (a) session timeout (minimum 20 min.) (b) the login account has been removed (c) the storage admin role of the login account has been removed
	16	C	C	-	V72-0063	Countermeasure against incorrect WEB status display on offline ENC firmware download	Just after starting "Offline ENC firmware download", messages "ENC microprogram download error detected(Unit-X)", "ENC#x microprogram download complete", and "ENC microprogram download complete" are displayed. The download status of WEB screen becomes yellow (executing) and then it becomes red (abnormal). After a while, message "ENC microprogram download complete" is displayed again and the download status becomes green (normal). ENC firmware download completes. <Equipment model> DF800H/M/S <Firmware version> V6.5/A(0865/A) or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (1) Offline ENC firmware download (Note: In General, ENC firmware is downloaded automatically online, if necessary.) (2) There exists the ENC whose firmware (ENC firmware) is the
	17	C	C	-	V72-0074	Countermeasure against the failure of PEL trace (= Physical Error Log of the expander in the backend)	Though a path failure occurred, PEL trace (= Physical Error Log of the expander in the backend) was not issued. <Equipment model> DF800H/M/S <Firmware version> V5.0 (0850/A) or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (1) A path failure occurred or periodical (by 30min.) collection of PEL trace (2) A path failure occurred and the (current) value of PEL differs to the value of PEL collected in the last time.

	18	C	C	-	V72-S004	Countermeasure against the phenomenon: scheduled shutdown is not processed even after 10 min from turning off the main switch on the front panel.	After the setting of DMLU for SnapShot and a blockade of a drive, planned shutdown is not processed even after 10 min from turning off the main switch on the front panel. <Equipment model> DF800H/M/S <Firmware version> First version or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (1) SATA HDD (2) A drive is blockaded (3) Random write to the RG which includes the blockaded HDD (4) planned shutdown (5) One of the following conditions occurs and the DDCB(Differential Data Control Block) is saved for the planned shutdown. 5.1 SnapShot P.P. is installed. 5.2 TCE P.P. is installed. 5.3 Shadow Image P.P. is installed and the pair status is either PSUS, PSUE or COPY. 5.4 TrueCopy P.P. is installed and the pair status is either PSUS, PSUE or COPY. 5.5 Dynamic Provisioning P.P. is installed. (6) DDCB Read/Write job generates dirty data (256MB to 8GB) is processed other than the HDD blockaded and the dirty data does
	19	C	C	-	V72QA010	Countermeasure against the failure on E-mail alert transmission	"Array Warning" E-mail Alert is not sent. ("Array Warning" should be sent when the status of the subsystem becomes from Ready to Warning.) <Equipment model> DF800H/M/S <Firmware version> 0870/A or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (1) E-mail alert is set up. (2) The status of the subsystem becomes from Ready to Warning. (Errors on SNMP, Firmware update, WEB, parity rebuild, DMLU, system area, Cache Residency Manager, LUN/LRC/LBA
	20	C	C	-	V72QA011	[Dynamic Provisioning] Countermeasure against the difference between the displayed value of DP pool usage and that of virtual LU usage during ShadowImage pair copy.	During ShadowImage pair copy, the followings are different and the difference is increasing: (1) the displayed value of DP pool usage and (2) the displayed value of virtual LU usage. <Equipment model> DF800H/M/S <Firmware version> 0870/A or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (1)DF800H/M/S, Firmware Version 0870 (2)HDP P.P. and ShdowImage P.P. are enabled (3)DP volumes are assigned to ShadowImage pair (4)ShadowImage pair copy
	21	C	C	-	V72-B012	[Dynamic Provisioning] Countermeasure against the insufficiency on the cascading check of True Copy and ShadowImage 1:N including virtual LU	(a) P-Vol and S-VoL of ShadowImage are normal LUs. (b) Creating TrueCopy pair, where the S-Vol of ShadowImage is assigned to the P-Vol of the TrueCopy pair. After that, creating ShadowImage pair against the same P-VoL, where S-VoL is virtual LU, is not processed as an Error. <Equipment model> DF800H/M/S <Firmware version> 0870/A or later <Conditions of Occurrence> The problem may occur when all following conditions are met. <Environment> (1) ShadowImage P.P. is enabled. (2) TrueCopy P.P. is enabled. (3) Dynamic Provisioning P.P. is enabled. (4) P-Vol and S-Vol of ShadowImage are normal LU. (5) Creating TrueCopy pair, where S-Vol of (4) is assigned to the P-Vol of the TrueCopy pair. <Function> ShadowImage <Operations> (6) On P-VOL of (4), create (or create and split) ShadowImage
					V6.5/F, 0865/F		7/10/2009　138　None

V6.5, 0865/F Base System V6.5/E, 0865/E	1	C	A	DF800-53572(EUC1020523) ,DF800-53573(EUC1020998)	V72-0092 (V65-0133)	Countermeasure against the access lost during online firmware update with path failover	During online firmware update with path failover, SNM2 detects a session timeout of Account Authentication (DMEG000212) and the path online process on the controller where the firmware is just updated fails. And then when a firmware update for another controller is started, an access lost may occur. <Equipment model> DF800H/M/S, SA8x0 <Firmware version> x862/A or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (0) Dual controller (1) Account Authentication function is enabled. (2) HSNM2 server is connected to LAN port of both controllers. (3) Execute online firmware update with path failover (4) At (3), a mode where the path online is triggered by the HSNM2 operation is selected. In particular, "Yes" is selected at the following dialogue: "When the micro program replacement starts, the controller stops accepting any access from the host until the replacement completes. If you select YES, access from the host will be again possible right after you select the OK button on the message that will be displayed when replacement is completed. If you select NO, access from the host will be possible as soon as the micro program replacement completes and selecting the OK on the message will have no action", in the firmware download window of HSNM2 GUI– Advanced	
	2	C	B	-	V72QA020 (V65-0132)	Countermeasure against error responses for I/Os after the CTL blockade and the recovery	Error responses (04/4400 hardware error) are issued for I/Os after the CTL blockade and the recovery . - If connected to host, and if a failover software is used, the I/O will be processed on the other CTL after the failover. - If connected to DF or SA (by copy function), the pair will become PSUE or the path will be blockaded. - If connected to RAID (by UVM), the path will be blockaded. In case of firmware update (either nonstop or path failover) instead of CTL blockade, this issue doesnot occur. <Equipment model> DF800H/M/S, SA8x0 <Firmware version> x850/A or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (0) Connected to higher-level devices (hosts, DF or SA for copy: TC/TCE/SimpleDR, RAID for UVM) through Fibre Channel interface (1) Plural write I/Os from higher-level devices are processed by Active-Active (cross-call among CTLs). (2) Then the CTL where receiving write I/Os is blockaded. (3) Then the CTL of (2) recovers. (4) Then plural write I/Os from higher-level devices are processed by Active-Active (cross-call among CTLs).	
	3	C	C	-	V65-0131	Countermeasure against an incorrect spin-up of HDDs from health-check command to the HDDs.	An HDD may spinup automatically, though no command to wake the HDD up is received. (The countermeasure modifies the interval to issue inquiries from CTLs.) <Equipment model> DF800H/M/S <Firmware version> The first version or later <Conditions of Occurrence> The problem may occur when all following conditions are met. - Keep SATA HDD be the spin-down (by Power Saving P.P. or by the shutdown)	
	V7.2/B, 0872/B							7/23/2009	140 None
V7.2, 0872/B Base System V7.2/A, 0872/A	1	I	-	-	V72-0087	Watch potential bugs for HDP table destruction and if the destruction occurs, fix it automatically by firmware itself	On the subsystem power off, the firmware verifies the HDP table and fix the table if necessary.		
	2	I	-	-	V72-0095	Information of RADIUS (for Account Authentication) is removed from Audit Log.	The RADIUS (for Account Authentication) support is canceled on V7.2/B.		

0872/A	3	C	A	DF800-53572(EUC1020523),DF800-53573(EUC1020998)	V72-0092	Countermeasure against the access lost during online firmware update with path failover	During online firmware update with path failover, SNM2 detects a session timeout of Account Authentication (DMEG000212) and the path online process on the controller where the firmware is just updated fails. And then when a firmware update for another controller is started, an access lost may occur. <Equipment model> DF800H/M/S, SA8x0 <Firmware version> x862/A or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (0) Dual controller (1) Account Authentication function is enabled. (2) HSNM2 server is connected to LAN port of both controllers. (3) Execute online firmware update with path failover (4) At (3), a mode where the path online is triggered by the HSNM2 operation is selected. In particular, "Yes" is selected at the following dialogue: "When the micro program replacement starts, the controller stops accepting any access from the host until the replacement completes. If you select YES, access from the host will be again possible right after you select the OK button on the message that will be displayed when replacement is completed. If you select NO, access from the host will be possible as soon as the micro program replacement completes and selecting the OK on the message will have no action", in the firmware download window of HSNM2 GUI– Advanced			
	4	C	B	-	V72QA021	Countermeasure against the CTL blockade on the removing the HDP pool by HSNM2	The CTL blockade occurs on the removing the HDP pool by HSNM2. <Equipment model> DF800H/M/S <Firmware version> 0872/A <Conditions of Occurrence> The problem may occur when all following conditions are met. (1)HDP P.P. is enabled. (2)Using HDP pool. (3)Some user operations on HDP pool or virtual LU on the HSNM2. (4)A logic of HDP.in the firmware modifies the table is modified. (5)Another logic of HDP in the firmware accesses the table on (3)			
	5	C	B	-	V72QA020	Countermeasure against error responses for I/Os after the CTL blockade and the recovery	Error responses (04/4400 hardware error) are issued for I/Os after the CTL blockade and the recovery . - If connected to host, and if a failover software is used, the I/O will be processed on the other CTL after the failover. - If connected to DF or SA (by copy function), the pair will become PSUE or the path will be blockaded. - If connected to RAID (by UVM), the path will be blockaded. In case of firmware update (either nonstop or path failover) instead of CTL blockade, this issue doesnot occur. <Equipment model> DF800H/M/S, SA8x0 <Firmware version> x850/A or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (0) Connected to higher-level devices (hosts, DF or SA for copy: TC/TCE/SimpleDR, RAID for UVM) through Fibre Channel interface (1) Plural write I/Os from higher-level devices are processed by Active-Active (cross-call among CTLs). (2) Then the CTL where receiving write I/Os is blockaded. (3) Then the CTL of (2) recovers.			
	V7.2/D, 0872/D							8/31/2009	149	None
V7.2, 0872/D Base System V7.2/B, 0872/B	1	C	A	DF800-53376(EUC964020)	V72-0102	Countermeasure against firmware update failure on the subsystem that the value of subnet mask is 0.0.0.0	When updating firmware on the subsystem that the value of subnet mask of management LAN is 0.0.0.0, the update fails. Then the controller is blockaded after rebooting. The controller does not recover even it is replaced. Or the controller is blockaded when the subsystem is rebooted after 0.0.0.0 was set to subnet mask of management LAN. (If the values of subnet mask of both controllers were 0.0.0.0, the subsystem does not become "Subsystem Ready".) <Equipment model> DF800H/M/S, SA8x0, <Firmware version> Version 0860/A or later <Conditions of Occurrence> The problem may occur in each case: Case (a) The failure may occur when the followings conditions are met. (1) The firmware version is less than V6.0/A. (2) The value of subnet mask of management LAN is 0.0.0.0. (3) Update the firmware to V6.0/A or later. Case (b) The failure may occur when the followings conditions are met. (1) The firmware version is V6.0/A or later. (2) Set 0.0.0.0 to the value of subnet mask of management LAN. (3) Reboot the subsystem			

	2	C	A	None	V75QA007, V72QA024	Countermeasure against the controller blockade with "Microprogram error[RSM]" when CoW SS or TCED is disabled or locked and after the start up of the subsystem.	With Dynamic Provisioning, if the operator disable CoW SS or TCED, cut off the power supply and put on the power supply, then after the next subsystem boot, the control information of Dynamic Provisioning become inadequate. Based on the inadeauate information, the Dynamic Provisioning process will cause one of the follwoings: (1) Subsystem down: The controller is blockaded and then the other controller is blockaded, too. (2) Memory destruction or user data lost, caused by the wrong information. <Equipment model> DF800H/M/S <Firmware version> Ver. 0870/A or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (1) Dynamic Provisioning is enabled (2) Cow SnapShot or True Copy Extended Distance is enabled (3) Then disable or lock both CoW SS and TCED. But do not execute the planned shutdown. (4) Cut off the power and then put on the power, without the cache volatilization.
	3	C	A	None	V72-0103	Countermeasure against the problem: With CPM enabled, enabling HDP, changing CPM configuration after PS cut off with cache memory volatile, and reboot, the subsystem will not boot up.	The subsystem will not boot up or will not process I/O without error messages. <Equipment model> DF800H/M/S <Firmware version> Ver. 0870/A or later <Conditions of Occurrence> The problem may occur when all following conditions are met. 1. CPM (i. e. Cache Partition Manager) is enabled 2. Then enable HDP (i. e. Dynamic Provisioning) 3. Then cut off the power supply of the subsystem with cache volatile (e. g. controller put off and plug in). 4. Then power on the subsystem 5. Then change the configuration of CPM (e. g. change the sub-partition). Be sure to use all the user area of cache memory. 6. Then PS OFF. 7. Then PS ON. Then, the usage of cache memory become inadequate and the subsystem will not boot up or will not process I/O.
	4	C	B	None	V72-0098(V62-0098)	Countermeasure against the problem: path failover by HSRP(Hot Standby Routing Protocol (Cisco™)) in a network segment is not available in iSCSI configuration.	Path failover by HSRP(Hot Standby Routing Protocol (Cisco™)) in a network segment is not available in iSCSI configuration which has redundant routers. <Equipment model> DF800H/M/S, SA8x0, <Firmware version> First version or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (1)iSCSI I/F (2)Redundant IP-SAN configuration by HSRP with Cisco's network router. (3)Some network failure occur. (Path failover is expected to be done.)
	5	C	C	D800-81153	V72-0099	Countermeasure against the inaccuracy of the drive operating rate on the Performance Monitor.	The drive operating rate displayed on the Performance Monitor is wrongly low for DF800H. <Equipment model> DF800H <Firmware version> First version or later <Conditions of Occurrence> (1) DF800H (2) Acquire the information of the drive operating rate on the Performance Monitor

	6	C	C	None	V80-0046	Countermeasure against the wrong blockade of a controller "Microprogram error[ERR]" by the frequent transfer error.	When transfer length error occur frequently in plural HDDs and the occurrence of the error on a controller beyond the predetermined threshold, the controller should be determined to be the cause and be blockaded with "Backend error count of the CTL was over the threshold[CODE-29](CTL-xx)". But the controller is blockaded with "the Controller is blockaded with Web message "Microprogram error[ERR]". <Equipment model> DF800H/M/S, SA8x0 <Firmware version> Ver. x862/A or later <Conditions of Occurrence> The problem may occur when all following conditions are met. - Failures (of HDDs and controllers) which the firmware will increase the error threshold counter on HDDs and controllers occur frequently.			
	V6.5/G, 0865/G							9/8/2009	151	None
V6.5, 0865/G Base System V6.5/F, 0865/F	1	C	B	R600/D800-24219(SD2809781)	V65-0137, V65-0138	Reduction of CPU utilization when the load of I/O is very high.	Firmware bug. Because the overhead increses for cache segment lock process between dual cores. <Details> (a) The free segments is shared by Xcore and Ycore. So, the firmware processes the exclusion when the free segments are used or discharged. Normally, the cache segment lock between Xcore and Ycore hardly occur at the same time, so the impact is not critical. But the cache segment lock between Xcore and Ycore cause collisions frequently because many free segments are discharged in parity generation when the I/Os are longer length and random write. (b) When the load of drives are very high, though data transfers to/from drives are started but they can not processed actually. The retry of them make the CPU busy. So, the overhead increases unreasonably and rapidly. (The countermeasures are: (a) Introduce intermediate queues to reduce the overheads by collisions between CPU cores. (b) Restrict the number of data transfers when the load of drives are very high.) <Equipment model> DF800H <Firmware version> First version or later <Conditions of Occurrence> The problem may occur when all the following conditions are met.			
	V6.5/H, 0865/H							9/14/2009	152	None
V6.5, 0865/H Base System V6.5/G, 0865/G	1	C	B	None	C090804266 (V65-0134, V65-0135)	Countermeasure against irrelevant blockade of plural HDDs (instead of ENC).	In some cases, though a path failure occurs in an ENC, the firmware can not detect the failure part (I.e. the ENC) by path diagnosis and the firmware blockades plural HDDs. <Equipment model> DF800H/M/S <Firmware version> First version or later <Conditions of Occurrence> The problem may occur when the following condition is met. (1) The failure of backend hardware (i.e. SAS Expander in a ENC)			
	2	C	B	DF800-53658	V65-0139	Countermeasure against the TC path failure and the HDD access outage.	Command time out which does not recover automatically occur in the both path of TrueCopy. In this case, The path recovery action (reboot of the subsystem) was necessary. <Equipment model> DF800H/M/S <Firmware version> Ver4.0/A(0840/A) or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (1) Configuration: DF800H ... Pairs are created between the two CPU core in the same CTL. DF800M/S, SA8x0 ... Pairs are created between the CTLs and a path is blockaded. (2) I/O of TC or TCE: Initiator command is issued from both core through a port. (3) TC path: DF/SA can not receive the response of the initiator command by some failure of FibreChannel Switch, cables and/or the other node. As a result, ABTS and Reset PLOGI of Fibre Channel are retried 4 times and the path is blockaded with "Path			

	3	C	C	None	V65-0140	Countermeasure against the case: the blockade of failed HDD may be late.	After replacing a HDD because of the frequent timeout failure (3 timeouts in a minute) of the HDD, if the 3 timeouts occur in a minute on the new HDD, the new HDD is not blockaded. (The new HDD will be blockaded by the different reason: hourly timeout threshold over.) <Equipment model> DF800H/M/S <Firmware version> V6.5/A(0865/A) or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (1) Failure on just an HDD. (2) Because of (1), timeout occur 3 times on the HDD and the firmware blockade the HDD. (3) After (2), the HDD is recovered by the removal/insert of by the replacement. (4) After (3), the time out occurs on the HDD. (5) During the above, no other timeout does not occur on the other HDDs.		
	V7.2/E, 0872/E							9/18/2009	154	None
V7.2, 0872/E Base System V7.2/D, 0872/D	1	C	A	None	V72-0113(V80-0211)	Both CTLs are blockaded with "Microprogram error[RCH]", if recovering a DP pool during a page format caused by an LU shrink of a DP-VOL etc.	[Phenomena] Both CTLs are blockaded with "Microprogram error[RCH]", if recovering a DP pool during a page format caused by an LU shrink of a DP-VOL etc. <Equipment model> DF800H/M/S <Firmware version> Ver. 0870/A or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Dynamic Provisioning is enabled. (2) Execute LU shrink of a DP-VOL or operation (create, remove, etc.) of SI pair. (3) Recovering the DP pool where the DP-VOL of (2) belongs. [Cause] Due to the firmware bug about pool recovery. When initializing a DP pool by the pool recovery operation, some information is not initialized. As a result, the internal		
	2	C	A	None	V72-0115(V80-0235)	When using SI/CoW SS/TC/TCE/Dynamic Provisioning on DF800H, a planned shutdown will cause a subsystem down.	[Phenomena] When using SI/CoW SS/TC/TCE/Dynamic Provisioning on DF800H, a planned shutdown will cause a subsystem down with "H0F100 The destage of the management information of DP pool failed". <Equipment model> DF800H <Firmware version> First Version or later [Conditions of Occurrence] The problem may occur when (1) or (2) is met. (1) All (1-1) to (1-5) are met: (1-1) DF800H (1-2) A DM-LU exists. (1-3) CoW SS is enabled / or TCE is enabled / or a ShadowImage pair (COPY or PSUS) exists / or a TC pair (COPY, PSUS or PSUE) exits. (1-4) Lots of dirty data exist. (1-5) Executing a planned shut down or a reboot from HSNM2. (2) All (2-1) to (2-5) are met: (2-1) DF800H (2-2) Dynamic Provisioning is enabled. (2-3) One or more DP pool exists. (2-4) Lots of dirty data exist. (2-5) Executing a planned shut down or a reboot from HSNM2.		
	3	C	A	None	V72-0112, V72-0117	When CTLs have different versions of firmware, some data inconsistency on a CTL memory will be occur if a failure occur in the backend and a Read I/O to SATA HDD is issued.	[Phenomena] When CTLs have different versions of firmware, some data inconsistency on a CTL memory will be occur if a failure occur in the backend and a Read I/O to SATA HDD is issued. According to which data is inconsistent, CTL blockade, Subsystem down etc. will occur. <Equipment model> DF800H/M/S, SA8x0 <Firmware version> First Version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) CTLs have different versions of firmware. (e.g. during the firmware update) (2) A backend failure occurs. (As a result, CTLs become cross-call status.) (3) Read I/O to SATA HDD is issued. [Cause] Due to the firmware bug about the data transfer among the CTLs for the Read I/O to SATA HDDs. The data may be transferred to the wrong CTL and the data may be stored on the wrong memory		

	4	C	B	None	V72QA026	HDD is blockaded by an I/O after the recovery of a DP pool.	[Phenomena] HDD is blockaded by an I/O after the recovery of a DP pool. HDU errors will occur frequently. <Equipment model> DF800H/M/S <Firmware version> Ver. 0870/A or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Dynamic Provisioning is enabled. (2) Create a DP pool. (3) Before finishing the format of (2), execute the pool recovery of the pool. (4) I/O operation during or after the pool recovery of (3). [Cause] Due to the firmware bug about the management of the internal
	5	C	B	R600/D800-24219(SD2809781)	V65-0137, V65-0138	Reduction of CPU utilization when the load of I/O is very high.	Firmware bug. Because the overhead increses for cache segment lock process between dual cores. <Details> (a) The free segments is shared by Xcore and Ycore. So, the firmware processes the exclusion when the free segments are used or discharged. Normally, the cache segment lock between Xcore and Ycore hardly occur at the same time, so the impact is not critical. But the cache segment lock between Xcore and Ycore cause collisions frequently because many free segments are discharged in parity generation when the I/Os are longer length and random write. (b) When the load of drives are very high, though data transfers to/from drives are started but they can not processed actually. The retry of them make the CPU busy. So, the overhead increases unreasonably and rapidly. (The countermeasures are: (a) Introduce intermediate queues to reduce the overheads by collisions between CPU cores. (b) Restrict the number of data transfers when the load of drives are very high.) <Equipment model> DF800H <Firmware version> First version or later <Conditions of Occurrence> The problem may occur when all the following conditions are met.
	6	C	B	None	C090804266 (V65-0134, V65-0135)	Countermeasure against irrelevant blockade of plural HDDs (instead of ENC).	In some cases, though a path failure occurs in an ENC, the firmware can not detect the failure part (I.e. the ENC) by path diagnosis and the firmware blockades plural HDDs. <Equipment model> DF800H/M/S <Firmware version> First version or later <Conditions of Occurrence> The problem may occur when the following condition is met. (1) The failure of backend hardware (i.e. SAS Expander in a ENC)
	7	C	B	DF800-53658	V65-0139	Countermeasure against the TC path failure and the HDD access outage.	Command time out which does not recover automatically occur in the both path of TrueCopy. In this case, The path recovery action (reboot of the subsystem) was necessary. <Equipment model> DF800H/M/S <Firmware version> Ver4.0/A(0840/A) or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (1) Configuration: DF800H ... Pairs are created between the two CPU core in the same CTL. DF800M/S, SA8x0 ... Pairs are created between the CTLs and a path is blockaded. (2) I/O of TC or TCE: Initiator command is issued from both core through a port. (3) TC path: DF/SA can not receive the response of the initiator command by some failure of FibreChannel Switch, cables and/or the other node. As a result, ABTS and Reset PLOGI of Fibre Channel are retried 4 times and the path is blockaded with "Path

	8	C	C	None	V65-0140	Countermeasure against the case: the blockade of failed HDD may be late.	After replacing a HDD because of the frequent timeout failure (3 timeouts in a minute) of the HDD, if the 3 timeouts occur in a minute on the new HDD, the new HDD is not blockaded. (The new HDD will be blockaded by the different reason: hourly timeout threshold over.) <Equipment model> DF800H/M/S <Firmware version> V6.5/A(0865/A) or later <Conditions of Occurrence> The problem may occur when all following conditions are met. (1) Failure on just an HDD. (2) Because of (1), timeout occur 3 times on the HDD and the firmware blockade the HDD. (3) After (2), the HDD is recovered by the removal/insert of by the replacement. (4) After (3), the time out occurs on the HDD. (5) During the above, no other timeout does not occur on the other HDDs.	
	9	C	C	D800-53631, DF800-24282	V72-0116	Unable to get SNMP MIB of the array	[Phenomena] In some case, the response to the SNMP MIB GET request is not issued from the array. <Equipment model> DF800H/M/S, SA8x0 <Firmware version> First Version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) The array receives a connection request to TCP/199 port. (2) Just after (1), the TCP/199 port receives RST packet (i.e. TCP reset) and the connection of (1) is disconnected. (Port scan may cause (1) (2).) (3) After (2), no accesses to TCP/199 port are received. [Cause] Due to the firmware bug about SNMP port access. Though actual SNMP access is arrived at UDP/161port, internal function of the array uses UDP/161 and TCP/199 port. If an access to TCP/199 is received and the connection is disconnected just after that, the SNMP agent of the array waits the connection to TCP/199 port and the actual SNMP MIB request to UDP/161 port	
	V8.0/A, 0880/A							10/22/2009	160	None
V8.0, 0880/A Base System V7.2/E, 0872/E	1	N	-	-	-	HDP Enhancement	HDP Enhancement is supported. - HDP pool optimization function (with Zero data reclamation) - Data Retention Utility function with HDP - Volume Migration function with HDP - Write Same command with only HDP			
	2	N	-	-	-	Replication Enhancement	Replication Enhancement is supported. - Shadow Image(P-Vol) – TrueCopy cascade - TrueCopy(S-Vol) – Shadow Image cascade			
	3	N	-	-	-	Dense RKA Enhancement (DF800S+3 RKAKXs)	DF800S supports three Dense RKAs.			
	4	I	-	-	-	LU Format data pattern changes to "zero" as default.	LU Format data pattern changes to "zero" as default for supporting zero data reclamation function.			
	5	I	-	-	-	Guard against DP-vol create operation and DP-vol expand operation when Over Provisioning Limit Threshold over.	Guard against DP-vol create operation and DP-vol expand operation when Over Provisioning Limit Threshold over.			
	6	I	-	-	-	Guard against SI pair create operation and resync operation when DP Pool Consumed Capacity Over.	Guard against SI pair create operation and resync operation when DP Pool Consumed Capacity Over.			
	7	I	-	-	-	Improvement of the usability of HSNM2 GUI on the display of both DP pool usage ration and Over Provisioning ratio.	Improvement of the usability of HSNM2 GUI on the display of both DP pool usage ration and Over Provisioning ratio.			
	8	I	-	-	-	The IO command response is changed, when DP Pool Consumed Capacity Over.	The IO command response is changed, when DP Pool Consumed Capacity Over.			
	9	I	-	-	-	DMLU should not be a selectable LU.	DMLU should not be a selectable LU.			
	10	I	-	-	-	Improvement of failure search accuracy of SAS controller firmware	Improvement of failure search accuracy of SAS controller firmware			

	11	C	A	None	V80-0206, V80-0281	Failure of reboot occurs and temporary sequential shutdown sequence stops when Auto Reboot(aureboot) is issued by SNM2 in case of controller blockade. And then, sequential shutdown is executed, controller is blockaded with Microprogram error[DMI] and subsystem down occurs.	[Phenomena] Failure of reboot occurs and temporary sequential shutdown sequence stops when Auto Reboot(aureboot) is issued by SNM2 in case of controller blockade. And then, sequential shutdown is executed, controller is blockaded with Microprogram error[DMI] and subsystem down occurs. <Equipment model> DF800H/M/S, SA8x0 <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)Controller is blockade. (No problem for Single controller configuration) (2)Auto Reboot is ordered. (3)Sequential shutdown is executed after failure of reboot ordering. (4)In sequential shutdown, the status is one of them below. - Snapshot key or TCE key is opened and DM-LU exists. - TrueCopy key or ShadowImage key is opened and pair status of "PSUS" or "COPY" or "PAIR" exist. - HDP key is opened and DP pool exists. - Volume Migration is executed. - Simple DR is executed (SA8x0) [Cause] Firmware bug.
	12	C	A	DF800-23452, DF800-53500	V80-0028, V72-0133, V72QA028	Subsystem can't detect worng connection of location of unit	[Phenomena] After subsystem was booted with wrong connection of the location of unit, multiple HDDs failed. After HDDs was recovered, multiple HDDs failure occurred on next array booting again. <Equipment model> DF800H/M/S <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) The ENC cable connection of unit which was created the RAID group fails during offline (2) Reboot the subsystem [Cause] Firmware bug. The lack of the wrong unit connection detection logic after RAID group creating.
	13	C	A	DF800-53736	V72-0149, V80-0337	Host Access can't be executed when firmware is exchanged in the system with SATA HDDs	[Phenomena] In case that the system has SATA HDDs and exchange of firmware or ENC replacement has done in the system, if power off and on hasn't be executed after exchange of firmware or ENC replacement, there is a possibility that host access can't be executed when next exchange of firmware is done. <Equipment model> DF800H/M/S, SA8x0 <Firmware version> Ver6.5/A(0865/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. A. Firmware version x865/A or later is used in the system. B. The system has SATA HDDs. C. Exchange of firmware or ENC replacement has done in the system. The last operation is one of the patterns below. (No problem if the last operation is that except the patterns below. Or, no problem if exchange of firmware or ENC replacement hasn't done in the system yet.) - Firmware exchange: x861/A or before -> x865/A or later x862/A – x865/A -> x865/B or later x865/B – x865/H -> x870/C or later x870/C -> x872/A or later - ENC replacement: Firmware version when ENC replacement has done is x865/A or later.

	14	C	B	None	V72-0142, V80QA044	Countermeasure against data loss which occurs after unexpected power off and cache data volatilization in HDP environment.	[Phenomena] There is a case that HDP mapping information isn't destaged to the drive in online. Data loss will occur about the data area related to non-destaged HDP mapping information after unexpected power off and cache data volatilization. <Equipment model> DF800H/M/S <Firmware version> 0870/A or later [Conditions of Occurrence] The failure occurs when the followings conditions are met. - HDP environment (Host I/O access is executed.) [Cause] Firmware bug. In HDP environment, HDP mapping information is periodically destaged to the HDDs in online. There is a bug that a mapping information isn't enqueued to destaging queue in specific updated timing of destaging queue. Except that cache data volatilization occurs, no problem if shutdown operation is executed because all
	15	C	B	None	V72-0136, V80-0316	Countermeasure against controller blockade with Microprogram error[HDP] in case that sequential read access is executed for S-VOL of PSUS(SP) pair (P-VOL: Normal LU, S-VOL: Virtual LU).	[Phenomena] A controller is blockaded with Microprogram error[HDP] in case that sequential read access is executed for S-VOL of PSUS(SP) pair (P-VOL: Normal LU, S-VOL: Virtual LU). <Equipment model> DF800H/M/S <Firmware version> 0870/A or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)Shadow Image with Quick Resync/Split mode (2)P-VOL: Normal LU (3)S-VOL: Virtual LU (4)Pair status is PSUS(SP) and there is data that hasn't copied from P-VOL to S-VOL yet. (5)Sequential read access is executed from S-VOL area that hasn't copied from P-VOL yet. [Cause] Firmware bug. In lookahead read, logical inconsistency occurs because firmware doesn't execute HDP address translation for LU type(Normal or Virtual) when lookahead read from S-VOL is executed after
	16	C	B	None	V72-0127, V80QA021 ,V80QA02 4	Countermeasure against increasing DP pool format time.	[Phenomena] DP pool format takes longer time. <Equipment model> DF800H/M/S <Firmware version> V7.0/A(0870/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)Pool format of plural DP RAID Groups are executed per each CPU core. (DP pool expansion or DP pool creation) (2)SATA HDD is installed. [Cause] Firmware bug. It takes long time for creation of pool format data because destage performance to SATA HDDs is low.
	17	C	B	DF800-23926	V80-0047	Countermeasure against DCTL time-out[H_PORT] in the timing of ABTS reset from the host.	[Phenomena] DCTL time-out[H_PORT] occurs in the timing of ABTS reset from the host. <Equipment model> DF800H/M/S <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when firmware receives ABTS from the host during data transfer. [Cause] Firmware bug There is a possibility that data transfer doesn't stop immediately when firmware aborts DMA transfer circuit for data transfer.

	18	C	B	None	V72-0120, V80-0062	Countermeasure against performance reduction of FC ports that are operated by the same CPU with wrong setting of FC port topology.	[Phenomena] Performance reduction occurs. Performance of FC ports that are operated by the same CPU with wrong setting of FC port topology is decreased. <Equipment model> DF800H/M/S <Firmware version> First version or later [Conditions of Occurrence] The problem occurs when all following conditions are met. (1)FC ports are used. (2)Topology setting of FC port is wrong. (3)I/O operation is executed to the FC port that is operated by the same CPU which operates FC port of (2). [Cause] Firmware bug. The processing time of normal I/O decreases because the process of the same failure notice event is executed repeatedly in case that link failure occurs continuously. <Countermeasure> Firmware neglects the same failure notice event in the specific interval.
	19	C	B	None	V72-0119, V80-0324, V73-0019, HDS-100	Countermeasure against controller blockade with Microprogram error[LSM] when firmware receives RSCN in I/O operation.	[Phenomena] Controller blockade occurs with Microprogram error[LSM] when firmware receives RSCN in I/O operation. <Equipment model> DF800H/M/S <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)Firmware receives RSCN. (2)One FC port connects to more than or equal 118 hosts. (3)The 118th host is HBA of HP or RAID External Storage/DF initiator. [Cause] Firmware bug. Firmware checks transfer initiator login status to decide response method in decoding process of receiving frame. There is a bug in the checking process and firmware executes the process as "check item exists" in spite of "check item doesn't exist". For this bug, firmware refers to illegal login management area and the controller
	20	C	B	DF800-53708	V72-0137, V80-0326	Countermeasure against controller blockade with Interface Board alarm.	[Phenomena] Controller blockade occurs with Interface Board alarm "H-IPC hardware error was detected(CTL-1,I/F-1)". Controller blockade occurs again after controller is swapped. <Equipment model> DF800H/M/S <Firmware version> V4.3/B or later [Conditions of Occurrence] V4.3/B or later [Cause] Firmware bug. Firmware doesn't support error status of "Data out of order" that is notified from interface controller chip in data-in phase. So firmware executes software reset because non-support error status is received. Controller is blockaded with threshold over in the environment in which a lot of "Data out of order" occurs.
	21	C	B	None	V72-0122, V80-0321	Countermeasure against controller recovery failure in case that the controller is blockaded before that recovery of ENC on unit0 about DF800H finishes when the ENC on unit0 is blockaded.	[Phenomena] Controller recovery failure about inserted controller occurs in case of the sequence from (1) to (4) below. X is the same number (0 or 1). (1)ENC X on Unit0 about DF800H is pulled out. (2)Controller X is pulled out. (3)ENC X on Unit0 is inserted (4)Controller X is inserted <Equipment model> DF800H/M/S <Firmware version> 0850/A or later [Conditions of Occurrence] The problem will occur when all following conditions are met. (1)DF800H (2)Controller X is blockaded by ENC failure (or pulled out) during Unit0-ENC X is blockaded (or pulled out). (3)Controller X is inserted after Unit0-ENC X recovered. (Unit0-ENC X should be recovered at first because controller recovery isn't executed during Unit0-ENC X blockaded.)

	22	C	B	None	V72-0124, V80QA025	Countermeasure against I/O performance reduction and illegal message repeatedly because route diagnostic of both backend path is executed repeatedly.	[Phenomena] I/O performance is reduced and illegal message is displayed repeatedly because route diagnostic of both backend path is executed repeatedly in case that HDD for current diagnostic target is blockaded during backend route diagnostic. <Equipment model> DF800H/M/S <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)Timeout of multiple SATA HDDs occur in the same backend path. (2)Backend diagnostic is executed. (3)HDD for current diagnostic target is blockaded between start of diagnostic for HDD and start of diagnostic for another backend path, about 5 seconds. [Cause] Firmware bug.
	23	C	B	None	V80QA026, V72-0134	Countermeasure against controller blockade with "Parity generation LA error[DRR]".	[Phenomena] Controller is blockaded with "Parity generation LA error[DRR]". <Equipment model> DF800H/M/S <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)The backend route failure occurred . (2)SAS controller Firmware fails query task command. [Cause] SAS controller Firmware bug. Because SAS controller Firmware have a bug of error recovery of query task command, SAS controller Firmware respond good response in spite of not transfer the data.When firmware executes parity generation from the data that is expected correct data on the cache, controller is blockaded by failure of parity generation circuit because the data isn't expected data and LA error occurs.
	24	C	B	None	V80-0262	Countermeasure against controller blockade with Microprogram error[CCP] when host read from P-VOL or S-VOL is executed during Shadow Image copy.	[Phenomena] Controller is blockade with Microprogram error[CCP] when host read from P-VOL or S-VOL is executed during Shadow Image copy. <Equipment model> DF800H/M/S <Firmware version> V7.0/A or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)Both P-VOL and S-VOL of Shadow Image are HDP virtual VOL. (2)Status of Shadow Image is "COPY" or "COPY-R(Restore)". (3)Source of Copy: HDP page non-assigned Source of Destination: HDP page non-assigned (4)Host read is executed from P-VOL or S-VOL [Cause]
	25	C	B	None	V80-0262	Countermeasure against controller blockade with Microprogram error[CCP] when host read from P-VOL or S-VOL is executed during Shadow Image copy.	[Phenomena] Controller is blockade with Microprogram error[CCP] when host read from P-VOL or S-VOL is executed during Shadow Image copy. <Equipment model> DF800H/M/S <Firmware version> V7.0/A or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)Both P-VOL and S-VOL of Shadow Image are HDP virtual VOL. (2)Status of Shadow Image is "COPY" or "COPY-R(Restore)". (3)Source of Copy: HDP page non-assigned Source of Destination: HDP page non-assigned

	26	C	B	None	V80-B019, V72-0143	Countermeasure against controller blockade with Microprogram error[RCH] when Shadow Image pair resync is executed in case that RG expansion is executed.	[Phenomena] Controller is blockaded with Microprogram error[RCH] when Shadow Image pair resync is executed in case that RG expansion is executed. HJ11OV Microprogram error[RCH] <Equipment model> DF800H/M/S <Firmware version> 0852/A or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)RG expansion is executed. (2)In case that one stripe row includes the area that is expanded. [Cause] Firmware bug. Firmware bug about process to execute changing the number of stripe before/after RG expansion. As a result, the firmware tries to			
	27	C	B	None	V72-0123, V80-0283	DF800H doesn't boot up in case that CUDG (diagnosis) error is detected about SAS controller.	[Phenomena] DF800H doesn't boot up in case that CUDG (diagnosis) error is detected about SAS controller. <Equipment model> DF800H <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)DF800H (2)CUDG error is detected about SAS controller. [Cause] Firmware bug. Firmware executes boot up sequence with synchronization among CPU cores. There is a bug that failure of synchronization occurs among CPU cores because CUDG timeout value for backend SAS			
	28	C	C	None	V80-0055, V72-0131	Countermeasure against illegal status indication(non blockaded) about HDP pool or virtual LU when HDP pool or virtual LU should be blockaded.	[Phenomena] When an information update is executed according with HDD failure, management status of pool isn't blockaded about pool or virtual LU when pool or virtual LU should be blockaded. <Equipment model> DF800H/M/S <Firmware version> V7.0/A or later [Conditions of Occurrence] The problem may occur when each following conditions are occurred. (1)When added HDD failure occurs in case of DP pool volume addition (included pool creation) (2)When HDD failure occurs in case that pool recovery is executed (3)When HDD failure occurs in case that virtual LU is created [Cause] Firmware bug. When LU or pool of HDP is operated, correct status isn't captured if HDP information is accessed from other CPU core with the			
	V7.2/G, 0872/G							10/23/2009	166	015
V7.2, 0872/G Base System V7.2/E, 0872/E	1	C	A	None	V72-0141	After CHK1, CTL blockade or power outage during the DP-Pool format, host I/O to the pool cannot be executed. (LA error will occur)	[Phenomena] After CHK1, CTL blockade or power outage during the DP-Pool format, host I/O to the pool cannot be executed. (LA error will occur) <Equipment model> DF800H/M/S <Firmware version> V7.0/A(0870/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Dynamic Provisioning P.P. is enabled (2) Pool Format of chunk or page (3) During (2), CHK1, CTL blockade or power outage occurs. (4) After (3), host I/O is processed. [Cause] Firmware bug. When CHK1/CTL blockade/power outage, the information of the formatting is cleared falsely The check of the start of pool format has a bug and the dirty data corresponding to the poor is discarded falsely. As a result, some areas in the pool are not formatted. Afterward, host I/O to the pool cannot execute as the data inconsistency. (LA error will occur.)			

	2	C	A	DF800-23452, DF800-53500	V80-0028,V72-0133,V72QA028	Subsystem can't detect wrong connection of location of unit	[Phenomena] After subsystem was booted with wrong connection of the location of unit, multiple HDDs failed. After HDDs was recovered, multiple HDDs failure occurred on next array booting again. <Equipment model> DF800H/M/S <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) The ENC cable connection of unit which was created the RAID group fails during offline (2) Reboot the subsystem [Cause] Firmware bug. The lack of the wrong unit connection detection logic after RAID group creating. <Countermeasure> 1. When subsystem detected the wrong connection of unit during booting , the subsystem does not boot. 2. Subsystem displays the web message that include the expected
	3	C	A	DF800-53736	V72-0149,V80-0337	Host Access can't be executed when firmware is exchanged in the system with SATA HDDs	[Phenomena] In case that the system has SATA HDDs and exchange of firmware or ENC replacement has done in the system, if power off and on hasn't be executed after exchange of firmware or ENC replacement, there is a possibility that host access can't be executed when next exchange of firmware is done. <Equipment model> DF800H/M/S, SA8x0 <Firmware version> Ver6.5/A(0865/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. A. Firmware version x865/A or later is used in the system. B. The system has SATA HDDs. C. Exchange of firmware or ENC replacement has done in the system. The last operation is one of the patterns below. (No problem if the last operation is that except the patterns below. Or, no problem if exchange of firmware or ENC replacement hasn't done in the system yet.) - Firmware exchange: x861/A or before -> x865/A or later x862/A – x865/A -> x865/B or later x865/B – x865/H -> x870/C or later x870/C -> x872/A or later - ENC replacement: Firmware version when ENC replacement has done is x865/A or later. D. Power off and on hasn't be executed after condition C. [Cause]
	4	C	B	None	V72-0142, V80QA044	Countermeasure against data loss which occurs after unexpected power off and cache data volatilization in HDP environment.	[Phenomena] There is a case that HDP mapping information isn't destaged to the drive in online. Data loss will occur about the data area related to non-destaged HDP mapping information after unexpected power off and cache data volatilization. <Equipment model> DF800H/M/S <Firmware version> 0870/A or later [Conditions of Occurrence] The failure occurs when the followings conditions are met. - HDP environment (Host I/O access is executed.) [Cause] Firmware bug. In HDP environment, HDP mapping information is periodically destaged to the HDDs in online. There is a bug that a mapping information isn't enqueued to destaging queue in specific updated timing of destaging queue. Except that cache data volatilization occurs, no problem if shutdown operation is executed because all data area is destaged to the HDDs. <Countermeasure> Exclusive processing is executed among enqueue/dequeue about destaging queue and HDP page information update.

	5	C	B	None	V72-0136, V80-0316	Countermeasure against controller blockade with Microprogram error[HDP] in case that sequential read access is executed for S-VOL of PSUS(SP) pair (P-VOL: Normal LU, S-VOL: Virtual LU).	[Phenomena] A controller is blockaded with Microprogram error[HDP] in case that sequential read access is executed for S-VOL of PSUS(SP) pair (P-VOL: Normal LU, S-VOL: Virtual LU). <Equipment model> DF800H/M/S <Firmware version> 0870/A or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)Shadow Image with Quick Resync/Split mode (2)P-VOL: Normal LU (3)S-VOL: Virtual LU (4)Pair status is PSUS(SP) and there is data that hasn't copied from P-VOL to S-VOL yet. (5)Sequential read access is executed from S-VOL area that hasn't copied from P-VOL yet. [Cause] Firmware bug. In lookahead read, logical inconsistency occurs because firmware doesn't execute HDP address translation for LU type(Normal or Virtual) when lookahead read from S-VOL is executed after lookahead read from P-VOL. <Countermeasure> Firmware executes HDP address translation for LU type(Normal
	6	C	B	None	V72-0127, V80QA021 ,V80QA02 4	Countermeasure against increasing DP pool format time.	[Phenomena] DP pool format takes longer time. <Equipment model> DF800H/M/S <Firmware version> V7.0/A(0870/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)Pool format of plural DP RAID Groups are executed per each CPU core. (DP pool expansion or DP pool creation) (2)SATA HDD is installed. [Cause] Firmware bug. It takes long time for creation of pool format data because destage performance to SATA HDDs is low. <Countermeasure> In case that SATA HDD pool format is executed, firmware decreases the number of issued command tags for pool format to execute destaging efficiently. The countermeasure is adapted to
	7	C	B	None	V72-0120, V80-0062	Countermeasure against performance reduction of FC ports that are operated by the same CPU with wrong setting of FC port topology.	[Phenomena] Performance reduction occurs. Performance of FC ports that are operated by the same CPU with wrong setting of FC port topology is decreased. <Equipment model> DF800H/M/S <Firmware version> First version or later [Conditions of Occurrence] The problem occurs when all following conditions are met. (1)FC ports are used. (2)Topology setting of FC port is wrong. (3)I/O operation is executed to the FC port that is operated by the same CPU which operates FC port of (2). [Cause] Firmware bug. The processing time of normal I/O decreases because the process of the same failure notice event is executed repeatedly in case that link failure occurs continuously. <Countermeasure> Firmware neglects the same failure notice event in the specific interval.
	8	C	B	None	V72-0119, V80-0324, V73C0019 01,HDS-100	Countermeasure against controller blockade with Microprogram error[LSM] when firmware receives RSCN in I/O operation.	[Phenomena] Controller blockade occurs with Microprogram error[LSM] when firmware receives RSCN in I/O operation. <Equipment model> DF800H/M/S <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)Firmware receives RSCN. (2)One FC port connects to more than or equal 118 hosts. (3)The 118th host is HBA of HP or RAID External Storage/DF initiator. [Cause] Firmware bug. Firmware checks transfer initiator login status to decide response method in decoding process of receiving frame. There is a bug in the checking process and firmware executes the process as "check item exists" in spite of "check item doesn't exist". For this bug, firmware refers to illegal login management area and the controller is blockaded with Microprogram error[LSM]. <Countermeasure> A result of decoding process is changed to "check item doesn't

	9	C	B	DF800-53708	V72-0137, V80-0326	Countermeasure against controller blockade with Interface Board alarm.	[Phenomena] Controller blockade occurs with Interface Board alarm "H-IPC hardware error was detected(CTL-1,I/F-1)". Controller blockade occurs again after controller is swapped. <Equipment model> DF800H/M/S <Firmware version> V4.3/B or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)iSCSI interface is used. (2)A router is used between host and DF. (3)Header or Data Digest for host packet is not used. [Cause] Firmware bug. Firmware doesn't support error status of "Data out of order" that is notified from interface controller chip in data-in phase. So firmware executes software reset because non-support error status is received. Controller is blockaded with threshold over in the environment in which a lot of "Data out of order" occurs. <Countermeasure> Firmware doesn't blockade the controller in case that interface controller chip detects error status of "Data out of order" in data-in phase.
	10	C	B	None	V72-0122, V80-0321	Countermeasure against controller recovery failure in case that the controller is blockaded before that recovery of ENC on unit0 about DF800H finishes when the ENC on unit0 is blockaded.	[Phenomena] Controller recovery failure about inserted controller occurs in case of the sequence from (1) to (4) below. X is the same number (0 or 1). (1)ENC X on Unit0 about DF800H is pulled out. (2)Controller X is pulled out. (3)ENC X on Unit0 is inserted (4)Controller X is inserted <Equipment model> DF800H/M/S <Firmware version> First version or later [Conditions of Occurrence] The problem will occur when all following conditions are met. (1)DF800H (2)Controller X is blockaded by ENC failure (or pulled out) during Unit0-ENC X is blockaded (or pulled out). (3)Controller X is inserted after Unit0-ENC X recovered. (Unit0-ENC X should be recovered at first because controller recovery isn't executed during Unit0-ENC X blockaded.) [Cause] Firmware bug. There is a bug that firmware can't recognize ENC of RKA when controller is inserted because firmware doesn't set the status of ENC port(Phy) on the controller "enable" in case that ENC of RKA is inserted after controller blockade.
	11	C	B	None	V72-0124, V80QA025	Countermeasure against I/O performance reduction and illegal message repeatedly because route diagnostic of both backend path is executed repeatedly.	[Phenomena] I/O performance is reduced and illegal message is displayed repeatedly because route diagnostic of both backend path is executed repeatedly in case that HDD for current diagnostic target is blockaded during backend route diagnostic. <Equipment model> DF800H/M/S, SA8x0 <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)Timeout of multiple SATA HDDs occur in the same backend path. (2)Backend diagnostic is executed. (3)HDD for current diagnostic target is blockaded between start of diagnostic for HDD and start of diagnostic for another backend path, about 5 seconds. [Cause] Firmware bug. There is a bug that abort timing of backend diagnostic doesn't exist in case that HDD for current diagnostic target is blockaded during backend diagnostic. So backend diagnostic for both paths is executed repeatedly. <Countermeasure>

	12	C	B	None	V80QA026, V72-0134	Countermeasure against controller blockade with "Parity generation LA error[DRR]".	[Phenomena] Controller is blockaded with "Parity generation LA error[DRR]". <Equipment model> DF800H/M/S, SA8x0 <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)The backend route failure occurred . (2)SAS controller Firmware fails query task command. [Cause] SAS controller Firmware bug. Because SAS controller Firmware have a bug of error recovery of query task command, SAS controller Firmware respond good response in spite of not transfer the data. When firmware executes parity generation from the data that is expected correct data on the cache, controller is blockaded by failure of parity generation circuit because the data isn't expected data and LA error occurs. <Countermeasure> The firmware detects the transfer count on good response and
	13	C	B	None	V80QA009	Countermeasure against sequential read performance reduction about S-VOL of Shadow Image (Quick Resync/Split).	[Phenomena] Countermeasure against sequential read performance reduction about S-VOL of Shadow Image (Quick Resync/Split). <Equipment model> DF800H/M/S <Firmware version> 0870/A or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)Sequential read is executed to S-VOL during PSUS(SP) of Shadow Image (Quick Resync/Split) after split. (2)Sequential read is executed from area to which firmware hasn't copy from P-VOL to S-VOL. [Cause] Firmware bug. There is a bug that the lookahead read isn't executed when sequential read is executed from P-VOL in case that lookahead read of S-VOL reached the area to which firmware hasn't copy from P-VOL. <Countermeasure>
	14	C	B	None	V80-B019, V72-0143	Countermeasure against controller blockade with Microprogram error[RCH] when Shadow Image pair resync is executed in case that RG expansion is executed.	[Phenomena] Controller is blockaded with Microprogram error[RCH] when Shadow Image pair resync is executed in case that RG expansion is executed. HJ11OV Microprogram error[RCH] <Equipment model> DF800H <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)RG expansion is executed. (2)In case that one stripe row includes the area that is expanded. [Cause] Firmware bug. Firmware bug about process to execute changing the number of stripe before/after RG expansion. As a result, the firmware tries to write HDDs wrongly and detects inconsistency of the process itself.
	15	C	B	None	V72-0123, V80-0283	DF800H doesn't boot up in case that CUDG (diagnosis) error is detected about SAS controller.	[Phenomena] DF800H doesn't boot up in case that CUDG (diagnosis) error is detected about SAS controller. <Equipment model> DF800H/M/S <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)DF800H (2)CUDG error is detected about SAS controller. [Cause] Firmware bug. Firmware executes boot up sequence with synchronization among CPU cores. There is a bug that failure of synchronization occurs among CPU cores because CUDG timeout value for backend SAS controller on the controller is too short. As a result, the controller is blockaded. <Countermeasure>

	16	C	B	D800-53718	V72-0139	CTL is blockaded with Microprogram error[ISM] on iSCSI login	[Phenomena] CTL is blockaded with Microprogram error[ISM] on iSCSI login <Equipment model> DF800H/M/S, SA8x0 <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) iSCSI I/F (2) Duplicate iSCSI Logins issued from the same host back to back. (If this failure occurs once per 24 hours, the CTL blockade will recover automatically by rebooting. But if this failure occurs more than once per 24 hours, the CTL blockade will not recover automatically.) [Cause] Firmware bug. Just after receiving an iSCSI Login command from a host, and if the duplicate iSCSI Login from the same host is received, the process for the 1st login should be aborted for 10ms. However, there is a bug in the abort process and that cause Microprogram error[ISM]
	17	C	B	None	V72-0147, V80-0336	iSCSI port is not available as the port is not link up.	[Phenomena] iSCSI port is not available as the port is not link up. <Equipment model> DF800H/M/S, SA8x0 <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) iSCSI I/F (2) An error occurs in an iSCSI protocol chip. (3) A CTL detects the error and execute reset process to the iSCSI I/F and another CTL also detects the error and executer reset process to the iSCSI I/F at the same time. [Cause] Firmware bug. Depending on the timing, a reset to the iSCSI I/F from a CTL and another reset to the iSCSI I/F, the reset is not executed actually. Then the recovery from reset is not done and as a result, the link goes down. <Countermeasure>
	18	C	C	None	V80-0055, V72-0131	Countermeasure against illegal status indication(non blockaded) about HDP pool or virtual LU when HDP pool or virtual LU should be blockaded.	[Phenomena] When an information update is executed according with HDD failure, management status of pool isn't blockaded about pool or virtual LU when pool or virtual LU should be blockaded. <Equipment model> DF800H/M/S <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when each following conditions are occurred. (1)When added HDD failure occurs in case of DP pool volume addition (included pool creation) (2)When HDD failure occurs in case that pool recovery is executed (3)When HDD failure occurs in case that virtual LU is created [Cause] Firmware bug. When LU or pool of HDP is operated, correct status isn't captured if HDP information is accessed from other CPU core with the processing in the individual timing from the operation. If HDD failure is recovery with replacement of HDD, this problem is recovered. <Countermeasure>
	V8.3/A, 0883/A						11/16/2009　171　None
V8.3, 0883/A Base System V8.0/A,	1	N	-	-	-	600GB SAS HDD support	600GB SAS HDD support
	2	N	-	-	-	Temperature monitoring support	Temperature monitoring support
	3	N	-	-	-	Failure factor indication of DP optimization is supported in HDP.	Failure factor indication of DP optimization is supported in HDP.
	4	I	-	-	-	Improvement of failure search accuracy of Expander hardware.	Improvement of failure search accuracy of Expander hardware.

0880/A	5	C	A	None	V83-0020,V72-0141	After CHK1, CTL blockade or power outage during the DP-Pool format, host I/O to the pool cannot be executed. (LA error will occur)	[Phenomena] After CHK1, CTL blockade or power outage during the DP-Pool format, host I/O to the pool cannot be executed. (LA error will occur) <Equipment model> DF800H/M/S <Firmware version> V7.0/A(0870/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Dynamic Provisioning P.P. is enabled (2) Pool Format of chunk or page (3) During (2), CHK1, CTL blockade or power outage occurs. (4) After (3), host I/O is processed. [Cause] Firmware bug. When CHK1/CTL blockade/power outage, the information of the formatting is cleared falsely The check of the start of pool format has a bug and the dirty data corresponding to the poor is discarded falsely. As a result, some areas in the pool are not formatted. Afterward, host I/O to the pool cannot execute as the data inconsistency. (LA error will occur.) <Action in the case of the failure> None. Please use the Firmware which includes the
	6	C	A	None	V80QA008	Subsystem down occurs when a lot of LU are formatted at a time.	[Phenomena] Subsystem down occurs by "H90320 Watch-dog time-out" when a lot of LU are formatted at a time. <Equipment model> DF800H/M/S <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. 1. A lot of LU are formatted at a time. 2. (LU number of #1) * (HDD number of RAID group) are bigger than 60240. [Cause] Firmware bug. Judgement process of Drive LED is repeated a lot when a lot of LU are formatted. Total time of this judgment process exceeds timeout (10 seconds). <Action in the case of the failure> None. Please use the Firmware which includes the countermeasure. To prevent this problem, please specify the number of LU formatted at a time for 1000 or less. <Countermeasure>
	6	C	B	None	V83-0029	Subsystem down occurs when the controller blockade or cache data non-volatilization after power off occurs on I/O access to virtual LU or pool rebalance in HDP environment.	[Phenomena] Subsystem down occurs when the controller blockade or cache data non-volatilization after power off occurs on I/O access to virtual LU or pool rebalance in HDP environment. <Equipment model> DF800H/M/S <Firmware version> V7.0/A(0870/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are occurred. (1)Dynamic Provisioning P.P. is enabled. (2)Access to management information about HDP pool is executed. (I/O, pool rebalance, or pool format, etc.) (3)controller blockade or cache data non-volatilization after power off occurs [Cause] Firmware bug. There is a bug about page queue changing sequence. Because recovery process from inconsistency status is insufficient, pool page status is inconsistent with queue status. <Action in the case of the failure> None. Please use the Firmware which includes the

	7	C	B	D800-53718	V83-0025,V72-0139	CTL is blockaded with Microprogram error[ISM] on iSCSI login	[Phenomena] CTL is blockaded with Microprogram error[ISM] on iSCSI login <Equipment model> DF800H/M/S, SA8x0 <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) iSCSI I/F (2) Duplicate iSCSI Logins issued from the same host back to back. (If this failure occurs once per 24 hours, the CTL blockade will recover automatically by rebooting. But if this failure occurs more than once per 24 hours, the CTL blockade will not recover automatically.) [Cause] Firmware bug. Just after receiving an iSCSI Login command from a host, and if the duplicate iSCSI Login from the same host is received, the process for the 1st login should be aborted for 10ms. However, there is a bug in the abort process and that cause Microprogram error[ISM]. <Action in the case of the failure> Dummy-replace the blockaded CTL or PS-OFF and ON. Then the
	8	C	B	None	V72-0147, V80-0336	iSCSI port is not available as the port is not link up.	[Phenomena] iSCSI port is not available as the port is not link up. <Equipment model> DF800H/M/S, SA8x0 <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) iSCSI I/F (2) An error occurs in an iSCSI protocol chip. (3) A CTL detect the error and execute reset process to the iSCSI I/F and another CTL also detect the error and executer reset process to the iSCSI I/F at the same time. [Cause] Firmware bug. Depending on the timing, a reset to the iSCSI I/F from a CTL and another reset to the iSCSI I/F, the reset is not executed actually. Then the recovery from reset is not done and as a result, the link goes down. <Action in the case of the failure> Dummy-replace the CTL whose port is not link up or PS-OFF and ON. Then the subsystem will recover. <Countermeasure>
	9	C	B	None	V83-0018	When power on the subsystem, a CTL is blockaded with a message "HJ13A3 Microprogram error[DSC]"	[Phenomena] When power on the subsystem, a CTL is blockaded with a message "HJ13A3 Microprogram error[DSC]" <Equipment model> DF800H/M/S, SA8x0 <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when ONE of following conditions is met. 1. PS-ON, ENC firmware download or non-stop firmware update 2. Adding trays or removing HDU/ENC/CTL when the subsystem is ready. 3. Failure on ENC/HDU, CHK1, CTL blockade, backend diagnosis [Cause] Firmware bug. When the reset process to HDU or ENC is executed, the end processing of the reset has a table search logic (of commands) with a bug. Then the firmware process the non-existing command in the table and as a result, the error occurs.. <Action in the case of the failure> None. Please use the Firmware which includes the

	10	C	B	None	V83-0021, V80QA021	CPU utilization rate becomes too high (more than 90%) during formatting the DPRG which consists of SATA HDDs.	[Phenomena] CPU utilization rate becomes too high (more than 90%) during formatting the DPRG which consists of SATA HDDs. <Equipment model> DF800H/M/S, SA8x0 <Firmware version> V7.0/A(0870/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Dynamic Provisioning P.P. is enabled (2) There are too many DPVOLs in the Array. (more than 2000 DPVOLs) (3) Executing more than 5 DP Pools formatting at the same time. [Cause] Firmware bug: The firmware executes some unnecessary checks in duplicated Host I/O transaction, so the CPU utilization rate becomes too high with relating to total LU numbers. (This problem was detected because generally, DPVOL may be created more than the Normal-LU.) <Recovery action to be taken in the problem> None. Please use the Firmware which includes the countermeasure. <Countermeasure>			
	V8.3/B, 0883/B							12/25/2009	180rev1	016
V8.3/B 0883/B Base System V8.3/A,	1	N	-	-	-	New HDD support	SAS SSD is supported.			
	2	N	-	-	-	New HDD support	2TB SATA HDD is supported.			
	3	C	A	DF800- 53806,53812,24760	V83-0036	Subsystem down by "BYTE-ENABLE error"	[Phenomena] When the HDP function is used, the subsystem might be downed by the following WEB message. [DCTL]The BYTE-ENABLE error of the slave command bridge was detected(CTL-x) x:Controller number <Equipment model> DF800H/M/S <Firmware version> V7.0/A(0870/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) HDP function use (2) When the following virtual LU accesses compete in the disk array. < host access 1> "Read/Write IO" is an access to the area where 32MB boundary was included. < host access 2> "Read/Write IO" is an access to the area where 32MB boundary is not included within the range of < host access 1>. Note : The controller is blockaded by occurrence of the condition. Therefore, when the condition is generated at both controllers, the subsystem is downed. [Cause] Firmware bug. In the resource release (stripe row release) processing, the release resource might not be able to be allocated in the resource waiting processing. As a result, the resource waiting time-out was generated and the illegal table reference happened.			
	5	C	B	-	V83-0038	Subsystem can not be booted up because both controllers are blockaded.	[Phenomena] Subsystem can not be booted up because both controllers are blockaded. Or I/O operation can not be executed because PIN is over when firmware exchange is executed or controller replacement(insertion) is executed in case that the system has a SATA HDD as system HDD. <Equipment model> DF800H/M/S, SA800/810 <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. [Not booted up] (1) Both device discover process (discover) on one backend path and request for device discover process on another backend path occur. [I/O operation cannot be executed.] (1) The system has a SATA HDD as system HDD. (2) Both device discover process (discover) on one backend path and request for device discover process on another backend path occur. [Cause] Firmware bug. Exclusive process about common flag doesn't be executed between controllers. So device discover process doesn't complete for illegal update.			
	V8.5/A, 0885/A							12/26/2009	182	017

V8.5/A 0885/A Base System V8.3/B,	1	I	-	HDS-099	-	Improvement of failure search accuracy against the illegal access from a firmware of a CTL to the other CTL that causes "[DCTL]The bridge error was detected[external access]."	Improvement of failure search accuracy against the illegal access from a firmware of a CTL to the other CTL that causes "[DCTL]The bridge error was detected[external access]."	
	2	I	-	DF800-53572, DF800-53573	-	Improvement of the check process of the firmware update.	Improvement of the check process of the firmware update.	
	3	I	-	-	-	"SATA Write & Compare" check (or SATA RAW) can be disabled or enabled by HSNM2 regardless of "SATA Write & Compare off" license.	"SATA Write & Compare" check (or SATA RAW) can be disabled or enabled by HSNM2 regardless of "SATA Write & Compare off" license.	
	4	I	-	-	-	Improvement of failure search accuracy of backend diagnosis.	Add the SAS address consistency check between SAS expander firmware, controller and ENC.	
	5	I	-	-	-	Improvement of DP Pool recovery speed.	Improvement of DP Pool recovery speed.	
	6	I	-	-	-	Improvement for the capturing dump data of iSCSI interface.	The dump data of iSCSI interface can be captured in a week without PS OFF/ON or firmware update.	
	7	I	-	-	-	DP page information is saved to drives at the firmware update.	DP page information is saved to drives at the firmware update.	
	8	I	-	-	-	Improvement of the response time when Queue full occurs frequently on FC interface.	Improvement of the response time when Queue full occurs frequently on FC interface.	
	9	I	-	-	-	Improvement of failure search accuracy of SAS controller firmware.	Improvement of failure search accuracy of SAS controller firmware.	
	10	C	A	None	V85-0035	HDD failure caused by LA/LRC errors	DF800-EN-M033 [Phenomena] In case that DF800 receives the read/write command from hosts, blockading multiple HDUs may occur with following messages. IY0F00 LA error (errcode:LUN) (Unit-x, HDU-y) IY0G00 LA error (errcode:LBA) (Unit-x, HDU-y) IY0H00 LRC error (Unit-x, HDU-y) x: Unit number, y: HDU number <Equipment model, Firmware version> DF800H, V6.2/A(0862/A) or V6.5/A to V6.5/H(0865/A to 0865/H) SA8x0, V5.0/A to V5.0/E(1850/A to 1850/E) [Conditions of Occurrence] The problem may occur when all following conditions are met. A.<In the case of DF800> Firmware version: 0862/A or 0865/A to 0865/H <In the case of SA8x0> Firmware version: 1850/A to 1850/E B.<In the case of DF800> The quick format command is ordered to a LU of more than 48TB (This applies to multiple LUs of more than 48TB specified, too.) <In the case of SA8x0> The quick format command is ordered to a LU of more than [Cause] Firmware bug. When the subsystem receives a sense command through the LAN while formatting LUs in the quick mode, an error relating to the sense command occurs and some spaces become unformatted.(transfer information that is supposed to be held in the local memory is mistakenly held in the quick format managing table in the cache memory.)As a result, when read/write come to the unformatted spaces, several HDD failures are falsely detected by LA/LRC errors. <Countermeasure> Fix the bug on the table management in the quick format processing. <Action in the case of the failure> Procedure-1: Back up the LUs including HDDs where LA/LRC errors have been found. Procedure-2: To re-format the LUs that include the blockading HDDs. Operator can identify the LUs by HSNM2 with following steps. (1) To identify RG number in "Assigned Drives" tab of "RG property". (2) To identify LU number in "Local Unit" tab of "RG property".	
	11	C	A	None	V83-0044	When CoW Snap Shot(CoW)/True Copy Extended Distance (TCE) pairs were released and controller blockade/Power Supply outage occurred, subsystem down or malfunction might occur.	[Phenomena] When CoW Snap Shot(CoW)/True Copy Extended Distance (TCE) pairs were released, controller blockade or subsystem down was generated and the following phenomena might be generated (1) Subsystem down occurs. (2) Illegal display of quantity consumed of pool and ratio consumed of pool. (3) The Web message "the number of Pool users threshold is over" is displayed illegally. (4) PSUE transition of pair of COW/TCE/SDR (5) The cycle trace information of TCE is illegal. (6) The character string of the Web message becomes illegal. (7) When iSNS is used for iSCSI interface, error "Micro Program Error [ILM]" is detected wrongly. <Equipment model> DF800H/M/S, SA800/810 <Firmware version> All version	

							[Conditions of Occurrence] The problem may occur when all following conditions are met. (1) CoW or TCE Program Product is enabled (2) CoW or TCE pair is existing. (3) Write IO is executed (4) Cow pair release with 1:1 or TCE pair release to which CoW and cascade are not done. (5) Within 30 hours after (4), Power Source outage or subsystem down occurs. [Cause] Firmware bug. Because the control information was updated illegally in cache at the error recovery opportunity(controller brocade or Subsystem down). <Countermeasure> Fix the bug in the update processing of the control information. <Action in the case of the failure>
	12	C	A	None	V85-0048	Subsystem down caused by the controller blockade when HDP is enabled.	[Phenomena] If a controller is blockaded (by the reason other than Power Supply failure) when HDP is enabled, the other controller may be blockaded too with a message "Microprogram error[HDP]". <Equipment model> DF800H/M/S <Firmware version> V7.0/A(0870/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) HDP is enabled (2) Power Source outage (without cache volatile) or controller blockade (other than Power Source failure) occurs [Cause] Firmware bug. The firmware manages chunk and page information of HDP as plural tables. When the controller is blockaded or Power Source outage occurs, such tables may become inconsistent according to the timing of the blockade/outage. Then the other controller which is not blockaded will recover from the inconsistency. However, this recovery process has a bug and the controller will be blockaded too. (This phenomenon does not occur at the controller blockade caused by Power Source failure.) <Countermeasure> Fix the bug in the recovery process when the tables of HDP information are inconsistent. <Action in the case of the failure> None.
	12	C	A	None	V85-0029	The subsystem may go down due to write failures of a DMLU accompanied by a controller failure during shutting down or rebooting the subsystem.	[Phenomena] The subsystem may go down due to write failures of a DMLU accompanied by a controller failure during shutting down or rebooting the subsystem. <Equipment model> DF800H/M/S <Firmware version> All version [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)When the subsystem is being shut down or when the subsystem is being rebooted. (2)A controller failure occurs while write operations to a DMLU are being implemented. [Cause] Firmware bug. When a controller failure occurs during shutting down or rebooting the subsystem, even if the controller failure does not affect write operations to a DMLU actually, the write operations are considered a failure and the subsystem goes down. <Countermeasure> Fix the bug in the recovery process from controller failure. <Action in the case of the failure> Power off and on.
	13	C	A	None	V85-0052	Subsystem down caused by Array booting after power cut without cache volatile while executing DP pool optimization.	[Phenomena] Subsystem down caused by Array booting after power cut without cache volatile while executing DP pool optimization. <Equipment model> DF800H/M/S <Firmware version> V8.0/A(0880/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. 1. Execute DP Optimization. 2. Array booting after power cut without cache volatile or controller blockade. [Cause] Firmware bug. Logical contradiction is occurred at the timing of Array booting after power cut without cache volatile or controller blockade during page migrating transaction in DP pool optimization. <Countermeasure> Fix the bug in the recovery process. <Action in the case of the failure> None.

	14	C	B	None	V85-0019	Array booting up failure in the Model upgrading process to DF800H.	DF800-EN-M031 [Phenomena] In the process of the Model upgrading to DF800H, Array booting up is failed. (Can't see the Ready status.) One controller failure (H90320 Watch-dog time-out) is occurred and another controller can not be accessed by LAN. <Equipment model> DF800H/M/S <Firmware version> V4.5/A(0845/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Cache Partition Manager Program Product is enabled. (2) Model upgrading from DF800S with 4GB/controller to DF800H with 8GB/controller. Or, Model upgrading from DF800M with 8GB/controller to DF800H with 8GB/controller, 10GB/controller or [Cause] Firmware bug. Generally in the model upgrade, the Firmware checks if the target Array has more than twice size from original Array and if not, rejects the operation. However, there are some missing cases which are actually unsupported configuration in this checking logic when 4GB-DIMM is used. In this problem, access to the memory area where actually does not exist causes the endless-loop and controller failure, so that you cannot see the Ready status. One controller is blocked for endless-loop. Another controller can not be accessed by LAN for endless-loop. <Countermeasure> Fix the bug in the checking logic of cache size of the model upgrade. <Action in the case of the failure> Please install additional cache memory to DF800H and retry the
	15	C	B	None	V85-0007	Plural ENC failures during Online Firmware Upgrading process.	[Phenomena] While in Online Firmware Upgrading, when one ENC is failed, then the other ENC in the same path may be also failed. (Firmware inappropriately blocks the other ENC.) <Equipment model, Firmware version> DF800H/M/S, V3.2/A(0832/A) or later SA8x0, All version [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) ENC Firmware Upgrading process is executed on plural ENCs in the same path. (Online Firmware Upgrading, or installing plural ENCs at the same time.) (2) While ENC reboot process in above (1), a certain link failure occurs. (3) Within 15ms from above (2), internal failure transaction [Cause] Firmware bug: Because of inappropriate transaction for link failure in ENC, the Firmware detects the normal ENC as failure. <Countermeasure> Fix above inappropriate logic in the Firmware. <Action in the case of the failure> Execute the dummy-replacing the ENC which is blocked inappropriately.
	16	C	B	None	V85-0009	Controller blockade with failure in the Local Memory.	[Phenomena] Controller blockade with failure in the Local Memory caused by Firmware logical contradiction. One of the following messages is issued at that time. [CSDS]The uncorrectable error on the write was detected[0xYYYYYYYY](CTL-X) [CSDS]The uncorrectable read memory error was detected[0xYYYYYYYY](CTL-X) The processor system bus error was detected[0xYYYYYYYY](CTL-X) <Equipment model> DF800H/M/S, SA800/810 <Firmware version> All version [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) 1bit error (ECC correctable error) in the Local Memory occurs. (2) 2bit error (ECC uncorrectable error) in the Local Memory [Cause] Firmware bug. Logical contradiction occurs when 1bit error (ECC correctable error) in the Local Memory occurs, then 2bit error (ECC uncorrectable error) in the Local Memory occurs. <Countermeasure> Fix above inappropriate logic in the Firmware. <Action in the case of the failure> Controller dummy-replacing or Array rebooting.

	17	C	B	None	V85-0022	Controller or ENC blockade with simultaneous occurrence of processor failure and backend failure.	[Phenomena] Controller or ENC blockade with simultaneous occurrence of processor failure and backend failure. <Equipment model> DF800H/M/S <Firmware version> V3.2B(0832/B) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Temporal processor failure occurs in the controller. (2) At the same timing of above (1), a certain Backend failure occurs in the other side of controller. [Cause] Firmware bug. Inappropriately judging the controller or ENC as failure. <Countermeasure> Fix above inappropriate logic in the Firmware. <Action in the case of the failure> Execute the dummy-replacing for their controller or ENC.
	18	C	B	None	V85-0033	When LU ownerships are changed for load balancing etc while commands are being executed, a copy operation , host I/O and reserve command may be error.	[Phenomena] When LU ownerships are changed like during load balancing while commands are being executed, a command error is detected, I/O operations cannot be executed or a reserve LU cannot be set. (a)Copy pair operations or a reserve command cannot be executed. (b)LUs become inaccessible to hosts for I/O. When a TrueCopy pare is created, the status of another LU at a remote site is changed to COPY status by mistake, so the host at the remote site becomes inaccessible for read/write. (c)A reserve LU cannot be set. Because another LU is reserved by mistake by Persistent Reserve OUT command, the specified LU cannot be reserved. <Equipment model> DF800H/M/S, SA800/810 <Firmware version> All version [Conditions of Occurrence] The problem may occur when all following conditions are met. [(a)A command error occurs] (1)A copy pair command is executed. (2)the ownership of the specified LU is changed. (like when load balancing occurs) (3)After the LU ownership has been changed, the LU receives a PIO related command(other than RD/WR) [(b)The host is inaccessible, (a)A command error occurs] (1)A True Copy pair command is executed (2)The ownership of the specified LU as the S-VOL by the command at the remote site is changed. (like when load balancing occurs) (3)After the LU ownership has been changed, the LU receives a PIO related command(other than RD/WR). [(c)The reserve information is wrong, (a) A command error occurs] (1)Persistent Reserve OUT command is executed (2)The ownership of the reserve LU is changed. (like when load balancing occurs) (3)After the LU ownership has been changed, the LU receives a PIO related command(other than RD/WR). [Cause] Firmware bug. There is a short period of time when changing a LU ownership is not prohibited, when a command has not been completed yet. When the ownership of a LU is changed during that short period of time, the buffer needed to execute the command is rewritten by the information of another command. <Countermeasure>
	19	C	B	None	V85-0037	A controller failure occurs after a host transfer DMA DCTL failure occurs during write operations	[Phenomena] A controller failure may occur due to a DMA DCTL failure during write operations. The message that is displayed when a controller is blockaded: Host transfer DMA error was detected(CTL-X,DMA-XX) <Equipment model> DF800H/M/S, SA800/810 <Firmware version> All version [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)iSCSI interface is used. (2)More than two write operations are issued with no read operations. (3)DCTL error by host write transfer occurs. [Cause] Firmware bug. When a host transfer DMA DCTL failure occurs during write operations, the iSCSI chip is not halted. So even when the DCTL has been recovered, the iSCSI chip still has been sending data to the DCTL and a data transmission error occurs. <Countermeasure> Reset the iSCSI chip at the recovery from DCTL failure. <Action in the case of the failure> Replace the blockaded controller with a new one.

	20	C	B	None	V85-0024	In HDP, dirty data of a virtual LU cannot be destaged to HDD because the Dirty Data Opportunity is inappropriately set.	[Phenomena] In HDP, dirty data of a virtual LU cannot be destaged to HDD because the Dirty Data Opportunity is inappropriately set. As a result, performance degradation in I/O may occur. In the worst case, I/O operations may be suspended. <Equipment model> DF800H/M/S <Firmware version> V7.0/A(0870/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)HDP is installed and enabled. A DP pool is set and a virtual LU is created. (2)Either the owner cores for a virtual LU and the DPRG or the partitions to which the CPM belong are different. (3)The Dirty Data Opportunity exceeds the threshold for facilitating de-staging Performance degradation: more than 8% I/O suspended: more than 10% (the initial value: 5%) (4)Any of the following behaviors are not found. The core for a virtual LU handles formatting the DP pool(chunks and pages) as well. The core for a virtual LU handles rebalancing the DP pool as well. [Cause] Firmware bug. There are some cases where the threshold for facilitating de-staging does not apply to virtual LUs. <Countermeasure> Decision processing for threshold for facilitating de-staging was modified. <Action in the case of the failure> Set the Dirty Data Opportunity lower than the threshold for facilitating de-staging.
	21	C	B	None	V85-0003	Controller blockade when controller executes internal retry (CHK1 reset).	[Phenomena] Controller is blockaded because of a factor "The read data parity error was detected in the register interface" when controller executes internal retry (CHK1 reset) in case that controller failure occurs. <Equipment model> DF800H/M/S, SA800/810 <Firmware version> All version [Conditions of Occurrence] The problem may occur when all following conditions are met. - Intermittent failure about CPU occurs in the controller. [Cause] Firmware bug. There is a bug about illegal detection of transfer error because data transfer doesn't abort unexpectedly when controller executes internal retry (CHK1 reset), in case that controller failure occurs. <Countermeasure> Occurrence of error is avoided by abort of data transfer with reset for backend protocol control IC. <Action in the case of the failure> Exchange of the blockaded controller
	22	C	B	None	V85-0041	Controller blockade with "Micro program error [RCH]"	[Phenomena] When CHK1 failure occurs at destination owner's controller during the LU owner switching, Micro program error [RCH] and controller blockade occurs. <Equipment model> DF800H <Firmware version> V4.6/A(0846/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)The LU owner is being switched by the instruction opportunity or the load balancing opportunity. [Cause] Firmware bug. The process which updated a local memory in another CPU core was leaked by recovered process of CHK1 failure. LU owner information mismatched on a cache memory and a local memory, and it was judged as logical contradiction. <Countermeasure> LU owner information is updated to another CPU core. <Action in the case of the failure> It is possible to recover in the blockage controller's dummy replacement or power supply OFF/ON in the disk array.
	23	C	B	None	V83-0042	Failure of ENC firmware download in the single controller mode fails.	[Phenomena] After the initial setup operation in single controller mode was executed, the download of the ENC firmware failed and the subsystem was ready (The ENC firmware is not updated). <Equipment model> DF800H <Firmware version> V8.0/A(0880/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Start-up in single controller mode (The single mode configuration) (2) Execution of ENC firmware download (The ENC firmware is

							[Cause] Firmware bug. The Link abnormal diagnosis and the ENC firmware download operate at the same time when LinkUp NG is detected by passing each other of internal processing before the unmount of the controller is detected at the start-up, and the ENC firmware download fails. The phenomenon was generated when the Link abnormal diagnosis operates had been changed with V8.0. <Countermeasure> In single controller mode, the unnecessary diagnosis processing is canceled. <Action in the case of the failure> None
	24	C	B	None	V85QA002	SNMP error and the device (subsystem) warning occur after firmware update.	[Phenomena] The SNMP error and the device (subsystem) warning state might occur after updating the firmware. The firmware update itself completes normally. "IB1700 SNMP RAM Device allocation error for SNMP :controller /STRC W3Q001 SNMP error occurred in the SNMP function(controller-1) :MANUAL/STRC" <Equipment model> DF800H/M/S, SA800/810 <Firmware version> All version [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Enable SNMP Program Product (2) Enable DHCP function (3) Update the firmware [Cause] Firmware bug. Because the SNMP information is checked unjustified when the DHCP function is used, and logical error has been detected. <Countermeasure> It is modified that SNMP information is not checked unjustified, when the DHCP function is used. <Action in the case of the failure> The device warning state can be canceled by the following operations. (1) Please disable SNMP Program Product. (2) After (1), please enable SNMP Program Product. The influence of this problem is the device warning state changing only.
	25	C	B	None	V85-0004	Some HDUs do not recover when HDUs are removed and installed continuously.	[Phenomena] Some HDUs do not recover when HDUs are removed and installed continuously. <Equipment model> DF800H/M/S <Firmware version> V8.3/A(0883/A) [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Remove and install plural HDUs continuously. [Cause] Firmware bug. Removing and installing plural HDU/ENC continuously, the HDU removal processing of the firmware is executed before the previous removal processing. Then the installation processing is executed though the backend-path is unavailable due to the removal processing. <Countermeasure> Fix the bug in the HDU removal processing. <Recovery when occurrence of phenomena> Remove and install HDUs one by one again.
	26	C	B	None	V85-0046, V90-0093	If a Power Supply outage occurs during HDP pool recovery, LA error (Logical Address error) for host I/O will occur after the subsystem's recovery.	[Phenomena] If a Power Supply outage occurs during HDP pool recovery, LA error (Logical Address error) for host I/O will occur after the subsystem's recovery. <Equipment model> DF800H/M/S <Firmware version> V7.0/A(0870/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) HDP Program Product is enabled (2) Order Pool recovery during HDP pool format (3) During the pool recovery of (2), the Power Supply outage occur (without cache volatile). (4) After the subsystem recovery of (3), LA errors (Logical Address errors) for host I/O will occur. [Cause] Firmware bug. There is a bug in the chunk management process of HDP. If the Power Supply is outage (without cache volatile) during the DP pool recovery processing, some part in a chunk will be remain as unformatted. If the host I/O accesses that chunk, LA error (logical address error) will occur. <Countermeasure> Fix the bug in the chunk management process. <Recovery when occurrence of phenomena> Please backup the user data, recover the pool and then restore the data from the backup.

	27	C	B	D800-81287	V85-0040	Due to the wrong port setting for HSNM2/HiCommand communication, the array can not respond to them.	[Phenomena] Due to the wrong port setting for HSNM2/HiCommand Secure communication, the array can not respond to them. <Equipment model> DF800H/M/S, SA800/810 <Firmware version> All Version [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Set the number of the Secure communication port of the array (default: 28355) to the Non Secure communication port from HSNM2 or HiCommand. (2) Packet lost occurs on the LAN between the HSNM2/HiCommand and the array. [Cause] Firmware bug. The start procedure of Secure communication has a bug such that the procedure cannot deal with the Non Secure communication request and the communication does not start. If such status holds several minutes, a packet with the timeout notice is sent from HSNM2/HiCommand to recover the procedure. However, if the packet is lost, the recovery will not be held. <Countermeasure> Fix the bug of the start procedure of Secure communication. <Recovery when occurrence of phenomena> Remove and install again the controller that cannot respond to the HSNM2/HiCommand. In addition, this issue does not affect to the other controller's ports and the ports to communicate to the hosts.	
	28	C	C	None	SSD-HD20	Illegal response from SSD (Solid State Disk)	[Phenomena] Illegal response 0B/4B06 (InitiatorResponseTimeOut) is issued from SSD (Solid State Disk) <Equipment model> DF800H/M/S <Firmware version> V8.3/A(0830/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) SSD is included. (2) IOs are issued to SSD. (3) Uncorrectable errors occur frequently in the SSD. [Cause] SSD Firmware bug. The bug in the update procedure of internal information in SSD will issue illegal error response (0B/4B06) when uncorrectable errors occur. <Countermeasure> Fix the update procedure of internal information in the SSD. <Countermeasure Firmware of SSD> AKS200: K007 --> K008	
	V8.5/B, 0885/B							1/19/2010　192
V8.5/B 0885/B Base System V8.5/A, 0885/A	1	C	B	DF800-24910	V85-0053	Access lost to the LU, which executed TC/TCE pair operation during remote path blockade.	[Phenomena] The following phenomenon may occur at MCU when TC/TCE pair operation has been executed during remote path blockade. (1) Access lost to the LU may occur, which executes pair operation command. (2) Pair operations may fail to the TC/TCE pair by SNM2. (3) Pair operations may fail to the TC/TCE pair by RAID Manager. (4) Reverse operation commands may fail to the TC/TCE pair from RCU. (5) Shutdown operation may not complete. <Equipment model> DF800H/M/S <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) TC or TCE is enabling. (2) A remote path is blockaded.	

							[Cause] The bug was found in the path alternation operation when TC/TCE pair operation command has been executed during remote path blockade. The micro-program bug may cause the alternation fail to the other CTL, and then the pair operation commands may be left and SNM2 or RAID Manager detects a time-out error. An access lost to the LUs, which the pair operation have been executed, occurs because host I/Os cannot be performed caused by the stay of the pair operation command. And also, operations of SNM2 and/or RAID Manager for all LUs fail. Host accesses to the other LUs are possible. <Countermeasure> Fix the path alternation operation for TC/TCE. <Action in the case of the failure> (1) Self-replacement of the CTL at MCU, which has or had the blockaded remote path. You can find whether the CTL had a blockaded remote path or not by Web message. Take action (2) after the problem cannot be resolved by the	
	2	C	A	-	V85-0053	The subsystem down occurs when TCE pair operation is performed with a path failure.	[Phenomena] TCE pair status changes improperly after TCE pair operation is performed with a path failure. As a result, the local subsystem down may occur due to "microprogram error [RVM]". <Equipment model> DF800H/M/S <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) TCE is enabling. (2) A remote path is blockaded. (3) TCE pair operation is performed to the CTL, which has the blockaded remote path, by SNM2 or RAID Manager. [Cause] Firmware bug The bug was found in the path alternation operation when TCE pair operation command has been executed during remote path blockade. The micro-program bug may cause the alternation fail to the other CTL, the TCE pair status may remain improperly . <Countermeasure> Fix the path alternation operation for TCE. <Action in the case of the failure> (1) Reboot the subsystem. (2) After (1), a CTL failure may occur due to a microprogram error [POM] when TCE pair operation is issued. TCE pair operations must not be issued if CTL failure occurs, . The subsystem down may occur when TCE pair operation is	
	3	C	A	-	V85-0053	When a CTL failure occurs and subsequently the CTL is recovered, TC/TCE pair status may change improperly.	[Phenomena] When a CTL failure occurs and subsequently the CTL is recovered, TC/TCE pair status may change improperly. As a result, (1)The pair status may change improperly to PSUE (2)The pair status may change improperly to PAIR (3)The local subsystem down may occur. <Equipment model> DF800H/M/S <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) TC/TCE is enabling. (2) A CTL failure occurs while TC/TCE pairs are in COPY status or TCE pairs are in PAIR status. (3) The CTL failure is recovered by replacing the CTL. (4) On CCI or SNM2, a TC/TCE pair operation command is	

							[Cause] Firmware bug. CTL switching operation fails when a TC/TCE pair operation command is executed with the CTL recovered. The CTL switching operation fails due to a firmware bug and the status of TC/TCE pairs in COPY or of TCE pairs in PAIR may change improperly.(How the pair status changes depends on the pair status when replacing the CTL. The subsystem down may occur in cases that the pair status is PSUS.) <Countermeasure> Fix the CTL switching operation for TC/TCE. <Action in the case of the failure> (1) When the status changes improperly to PSUE: Resynchronize the pairs. (2) When the status changes improperly to PAIR: Suspend the pairs and resynchronize them. (3) When the subsystem down occurs: - In the case of TC: Pull out both the cables for remote path, reboot the subsystem and then the pair status will change to PSUE automatically. After recovering the remote paths, resynchronize the pairs in PSUE. - In the case of TCE: (a) Pull out both the cables for remote path, reboot the subsystem and then the pair status will change to PSUE automatically. After recovering the remote paths, resynchronize the pairs in PSUE.			
	V8.5/C, 0885/C							2/12/2010	195	None
V8.5/C 0885/C Base System V8.5/B, 0885/B	1	C	A	D800-53907(EUC1115195), DF800-25094(SD3001135)	V85-0064, V85-0074, V85-0077	CTL blockade with Watch-Dog Time-out when DP pool is created.	DF800-EN-M037 [Phenomena] (1) When DP pool is created as 28D+2P, it takes 10sec or more for its processing, and the CTL is blockaded with "Watch-Dog Time-out". When the firmware version is V7.0 to V7.2/F, (2) The recovery operation for (1) fails and the DP pool can't be created. When the firmware version is V7.2/G to V8.5/B, (3) The DP pool creation fails by (1). On the other hand, the DP pool that can't be deleted is created. <Equipment model> DF800H/M/S <Firmware version> V7.0/A(0870/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) HDP is enabled (2) Creation, the capacity addition or the deletion of a DP pool is executed. (3) The DPRG capacity of (2) is 16TB or more. (Especially, when the user port and the maintenance port are connected in a local environment, Watch-dog time-out is generated easily) Note: The operation time is about 16TB/9sec and 6TB/3sec in [Cause] Firmware bug. (1) (When 16TB (8D+2P with 2TB HDD) DP pool is composed, the expected time is about 5sec in AMS2500 or about 9sec in AMS2300/2100.) (2) If the CTL blockade occurs during a DP pool creation, the creation fails. (3) Then the DP Pool information is inconsistent and it is impossible to delete the DP pool. <Countermeasure> (1) So as not to generate Watch-dog time-out, the firmware is modified. (2) The processing about retry is changed. (3) SNM2 displays failure of the pool and provides the delete operation of the pool. <Action in the case of the failure> When the firmware version is V7.0 to V7.2/F, please execute PS-OFF/ON. When the firmware version is V7.2/G to V8.5/B, please execute initial setup and create DPRG less than 16TB.			
	2	C	A	None	V85-0057	After the operation of shrinking DP-VOL Capacity, the subsystem down occurs with Microprogram error [HDP] on the both CTL.	[Phenomena] After the operation of shrinking DP-VOL Capacity, Microprogram error [HDP] occurs on each CTL. As a result, the subsystem down occurs. <Equipment model> DF800H/M/S <Firmware version> V7.0/A(0870/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) HDP is enabled (2) Shrinking the capacity of DP-VOL (3) It is not a boundary of 4GB in LU size after the shrinking operation the DP-VOL capacity. (4) After Shrinking the DP-VOL Capacity operation, the page state in the boundary 4GB is following (a) and (b). (a) Both the allocated page and the unallocated page are existed. (b) After all allocated pages are reduced beyond the limits of DP-VOL size.			

							[Cause] Firmware bug. An illegal state in an internal table is generated, then the subsystem down occurs by Microprogram error in both CTL. <Countermeasure> After shrinking DP-VOL, check all the page association in the 4GB area. If no page is associated, the linkage between the DP-VOL and the table is released. <Action in the case of the failure> None	
	3	C	A	None	V85-0058	Subsystem down caused by the failure such as CHK1, CTL blockade or power failure during HDP recovery process.	[Phenomena] The subsystem down is caused by CHK1, the CTL blockage, and power failure in the recovering operation, when HDD recovery or online verify or DP pool format or LU format is executed. <Equipment model> DF800H/M/S <Firmware version> V7.0/A(0870/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) HDP is enabled (2) HDD recovery at DP pool or online verify or DP pool format or LU format is executed. (3) When the failure (CHK1, the CTL blockage, and power failure(nonvolatile)) recovery is executed, the failure occurred. (4) When the HDD recovery in DP pool , the occurrence condition is (2) and (3). Because it retries automatically at the HDD recovery in the DP pool). [Cause] Firmware bug. When failure(the CTL blockage and power failure) occurs with the chunk lock status and transition of chunk status, there is a timing that the chunk state becomes illegal, and logical error is detected with both CTL and the system down occurs. <Countermeasure> When the illegal chunk status is detected, it doesn't connect it with the queue. <Action in the case of the failure> None	
	4	C	A	None	V85-0061	When the CHK1/CTL blockage is occurred while the DP pool operation, the system down is generated.	[Phenomena] There is a possibility that the following events occur when CHK1 or the CTL blockage is generated while updating DP pool information in the recovery, the deletion, and the RG blockade of the DP pool in the HDP configure. (1) It is impossible to save the HDP information and the data corruption is occurred with volatilizing. (2) The pool optimization is executed, and there is a possibility that the CTL blockage by the unjustified memory access. In this case, both CTLs are blockaded. (3) The pool optimization is executed, and its progress does not advance. <Equipment model> DF800H/M/S <Firmware version> V7.0/A(0870/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) HDP is enabled (2) When CHK1 or the CTL blockage is generated while updating DP pool information in the recovery, the deletion, and the RG [Cause] Firmware bug. When a failure recovery process Because the recovery processing didn't operate by the gap of the memory update timing of the DP pool processing, the information on cache memory and work memory become inconsistent. <Countermeasure> Before updating DP pool information, the DP pool information on cache memory is update by the DP pool information of work memory to keep consistency. <Action in the case of the failure> None	

	5	C	A	None	V85-0062	When LU format operation is executed, the subsystem down caused by power failure or CTL blockage.	[Phenomena] The subsystem down generates by "Watch-dog time-out", when PS/on with volatilizing or CTL blockage are occurred while DP-vol format is executed. <Equipment model> DF800H/M/S <Firmware version> V7.0/A(0870/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) The page allocated with total about 150TB or more in several DP-VOLs. (2) Format operation to several DP-VOLs (3) When CTL blockade or power failure occurred, failure recovery is executed. [Cause] Firmware bug. The process "Recount of page or chunk that has been allocated" takes longer time than expected. <Countermeasure> The recalculation is executed by each LU. <Action in the case of the failure> Please execute PS-ON with volatile.
	6	C	A	None	V85-0069	CTL communication send time-out is generated if another core issues the communication when DP-Vol operation is executed, and the CTL blockage is occurred.	[Phenomena] "CTL communication send time-out" is generated if another core issues the communication when DP-Vol operation is executed, and the CTL blockage is occurred. (When the pages are allocated with capacity of 3TB or more at Shrinking the DP-VOL Capacity. When the pages are reduced with capacity of 3TB or more at DP-VOL deletion and format.) <Equipment model> DF800H/M/S <Firmware version> V7.0/A(0870/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) When the DP-Vol operation(DP-Vol delete, format and Shrinking capacity) is executed for the large DP-vol. (When the pages are allocated with capacity of 3TB or more at Shrinking the DP-VOL Capacity. When the pages are reduced with capacity of 3TB or more at DP-VOL deletion and format.) (2) When processing at constant period communicates between [Cause] Firmware bug. DP-Vol operation with interrupt prohibited, and there is the case which it takes 3sec or more to release many pages. Because the communication interrupt cannot pick up by 3sec or more. Though the mask of interrupt is done and becomes "CTL communication send time-out" in the other core on the communication. <Countermeasure> Interrupt for the communication is permitted at DP-Vol operation (DP-Vol deletion, DP-Vol format, and DP-Vol reduction) with chunk and page releasing. <Action in the case of the failure> When shrinking the DP-VOL capacity, the operation separately for the number of bytes for less than 3TB is executed.
	7	C	B	DF800-25085(SD2987186)	V85-0068	TC/TCE CTG information is incorrectly cleared when SI/SS pair is deleted.	[Phenomena] CLI command "aureplicationmon -evwait" to TC/TCE pair or pair operations using Groupname gets error after SI/SS pair is deleted from SNM2. <Equipment model> DF800H/M/S <Firmware version> All version [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) There are SI or SS pairs in a CTG. (2) There are TC or TCE pairs in a CTG. (3) Delete all pairs of the SI or SS belonging to a CTG. (4) The CTG# of SI or SS pairs which deleted in (3), is smaller than CTG# of TC or TCE pairs. [Cause] Firmware bug. CTG information (Groupname etc.) of TC/TCE is incorrectly cleared when deleting SI/SS pairs. <Countermeasure> Fix the firmware bug described above. <Action in the case of the failure> Create a TC/TCE pair whose CTG# is the same one to the corrupted pair. (CTG information is recreated when creating pair.) Set the correct groupname.

	8	C	B	None	V85-0054	CTL is blockaded due to Microprogram Error[PRO] when the subsystem is turned off during online firmware upgrading.	[Phenomena] If the subsystem that mixed HDP support firmware and the non-support firmware between the CTLs is turned off, the message "Microprogram error[PRO]" is displayed, and then the CTL is blockaded. However the power-off is completed normally, and also the firmware update will be completed when the subsystem will start up next. <Equipment model> DF800H/M/S <Firmware version> V7.0/A(0870/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. - DM-LU is created. - Snapshot is enabled, or TCE is enabled, or SI pair that the status is "COPY" or "PSUS" have been created, or TC pair that the status is "COPY", "PSUS" or "PSUE" have been created, - A CTL has V6.5 or earlier firmware, and the other one has V7.0 and later firmware. [Cause] Firmware bug. Because the HDP support CTL issue a communication to the non-support CTL as an extension of saving data from cache to DM-LU on the drive during firmware are different between controllers, the communication fails and then the CTL is blockaded. <Countermeasure> The HDP support CTL does NOT issue a communication to the non-support CTL as an extension of saving data to DM-LU during firmware are different between controllers. <Action in the case of the failure> None.
	9	C	B	None	V85-0056	Reused capacity of data area about Data Provisioning doesn't increase after executing LU shrink because the chunk that may be released doesn't release. (In the worst case, reused operation starts after 24 hours from formatting completion.)	[Phenomena] If DP-VOL shrink or optimization of Data Provisioning pool is executed, the data area that may be reused doesn't be reused for long term. <Equipment model> DF800H/M/S <Firmware version> V8.0/A(0880/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. - HDP environment - When formatting of chunk is executed for pool creation/ pool recovery/ DP-VOL deletion/ DP-VOL formatting/ DP-VOL shrink. - There is a chunk that can be reused because DP-VOL shrink or [Cause] Firmware bug. When firmware searches the chunks that can be reused, firmware checks only the chunks that are formatted fully. So, the data area that may be reused doesn't be reused because firmware doesn't search the next of the chunk under formatting if there is a chunk under formatting, <Countermeasure> Firmware expands the range of searching chunks to all of the chunks that can be reused. <Action in the case of the failure> None.
	10	C	B	None	V85-0060	Unable to resolve Depletion alert status of HDP pool	[Phenomena] HDP caution status that must be resolved cannot resolved actually if failure occurs at the timing of cancellation about caution status because of decreasing used capacity after that the HDP status changes initial caution/ drained caution/ drained status when the capacity of HDP pool usage is over the threshold. <Equipment model> DF800H/M/S <Firmware version> V7.0/A(0870/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. - HDP environment - HDP pool is created and is used until the HDP status changes to initial caution/ drained caution/ drained status. - The capacity of HDP pool usage decreases under the threshold of caution (i.e. Depletion alert). - Failure or sequential shutdown occurs at the timing of cancellation about caution status (initial caution/ drained caution/ drained status). The failure is CHK1, controller blockade.

							[Cause] Firmware bug. If failure occurs at the timing between the clear of status notification flag and translation of pool status, pool status doesn't change from initial caution/ drained caution/ drained status to another status although status notification flag has already cancelled. <Countermeasure> Firmware supports recovery process from inconsistency status and executes the process completely not to occur information inconsistency when that failure occurs at the timing between the clear of status notification flag and translation of pool status. <Action in the case of the failure> None.
	11	C	B	None	V85-0063	If failure occurs in the timing of translation about chunk status, capacity value that can be assigned for HDP pool is incorrect.	[Phenomena] If failure (controller blockade of unexpected power off) occurs in the timing of assignment for new page, assigned capacity of chunks is incorrect. <Equipment model> DF800H/M/S <Firmware version> V7.0/A(0870/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. - HDP environment - Controller blockade or unexpected power off occurs [Cause] Firmware bug. When firmware checks the capacity of chunks again in the recovery process from inconsistency status, there is a bug about subtraction in the checking process. <Countermeasure> If the number of chunks is 0 when firmware counts the number of chunks, firmware doesn't execute subtraction. <Action in the case of the failure> Please execute power off and on.
	12	C	B	None	V85-0066	Subsystem down with "The destage of the management information	[Phenomena] Subsystem down with "The destage of the management information of DP pool failed" during shut-down. <Equipment model> DF800H/M/S <Firmware version> V7.0/A(0870/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) CoW ShapShot, TCE or HDP is enabled (2) PIN data exist. (3) Shut down or reboot the subsystem [Cause] Firmware bug. Saving the management information (for Cow SS/TCE/HDP) from the cache memory to HDDs does not work well when PIN data exist. <Countermeasure> Improve the destaging process of such information though PIN data exist. <Action in the case of the failure> None.
	13	C	B	None	V85-0072, V90-0045	CTL blockade when changing a topology of FC interface	[Phenomena] CTL blockade occurs by the failure of DCTL when changing a topology of FC interface. The Message "Host transfer DMA error was detected(CTL-X,DMA-XX)" is issued. <Equipment model> DF800H/M/S <Firmware version> V7.2/A(0872/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) 8Gbps FC(Fibre Channel) interface board (2) Processing Read I/O (by cross-call in the array) (3) The DMA error on the FC port of (2) [Cause] Firmware bug. Reset to the FC protocol chip interface (after the DMA error for the recovery from the error) is not executed eventually by the timing. <Countermeasure> Reset the protocol chip for the recovery without fault on any case of timing. <Action in the case of the failure> Replacing the CTL which is blockaded

	14	C	B	None	V85-0079	Persistent Reserve information is removed in the remote DF when creating a remote path.	[Phenomena] Persistent Reserve information is removed in the remote DF when creating a remote path. The Persistent Reserve information in the following LUs is deleted. SA8X0: 0 to 1349, DF800S: 0 to 970, DF800M: 0 to 1014, DF800H: 0 to 1088 <Equipment model> DF800H/M/S <Firmware version> V6.2/A(0862/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) The array is the remote side of TC/TCE remote path [Cause] Firmware bug. Persistent Reserve information in certain LUs in the remote array gets incorrectly cleared by the path health check process which is done once every minute when TC/TCE path has been created. <Countermeasure> Fix the problem in the process of remote path health check. <Action in the case of the failure> None
	15	C	B	None	V85-0073, V90QA009	Microprogram error[DSC] caused by the blockade of a CTL, PIN over and the PS-OFF/ON	[Phenomena] Microprogram error[DSC] caused by the blockade of a CTL, PIN over and the PS-OFF/ON <Equipment model> DF800H/M/S <Firmware version> V7.0/A(0870/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) HDP is enabled (2) Create a DP pool or growing the capacity of a DP pool. [Cause] Firmware bug. If a failure occurs during the update process of Chunks on creating/growing a pool, the process ends even though some Chunks are not updated, eventually. <Countermeasure> Fix the failure recovery process during the update process of Chunks. <Action in the case of the failure> None.
	16	C	C	DF800H-53885HE(EUC1102719), DF800M-53877(EUC1078591), DF800-25011(EUC1112124)	V85-0059	Firmware upgrading fails when Session-timeout length for Account Authentication is disabled.	DF800-EN-M036, SA800-EN-M036 [Phenomena] Online firmware upgrading fails with the following message. Even if you retry in accordance with the message, firmware update fails again. "DMEA00200E: Could not finish replacing the firmware. Confirm the subsystem status and the LAN environment, and then try again only the updating. Please try it again at least three times until complete it normally. If you cannot totally complete it normally, power OFF and then power ON the subsystem." <Equipment model> DF800H/M/S <Firmware version> All version [Conditions of Occurrence] The problem occurs when all following conditions are met. (1) Account Authentication is enabled. (2) Session-timeout length for Account Authentication is disabled. (3) Upgrading the firmware as online firmware update. [Cause] Firmware bug. When Session-timeout length for Account Authentication is disabled, some sessions are terminated in the reboot-process for updating firmware. As a result, session-timeout occurs on HSNM2, and firmware update fails. <Countermeasure> Fix the session management not to terminate the session wrongly after the reboot of CTL, when Session-timeout length for Account Authentication is disabled. <Action in the case of the failure> - Connect a LAN cable to controller 1 of the array. Then register the array to HSNM2 with the IP address of controller 1 only. Then select the array on HSNM2. - Or turn off the array and turn on it.

	17	C	C	DF800-53911(EUC1108664)	V85-0071	Wrong detection of Session-timeout of Account Authentication on HSNM2.	[Phenomena] Unable to do HSNM2 operation to DF800H where Account Authentication is enabled as the session-timeout occur soon after the log-in. DMEG100013: Current session has timed out. Please login again. <Equipment model> DF800H <Firmware version> All version [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) DF800H (2) Account Authentication P.P. is enabled. (3) Login to the DF800H with HSNM2 [Cause] Firmware bug. In the dual-core CPU on the DF800H CTL, the firmware of the core-X watches the HSNM2 session. Though the firmware of the core-Y should not watch the session, that watches the session practically and detects the time-out by the difference of the timers of the cores. <Countermeasure> Remove the check process of the session-timeout from the firmware of core-Y. <Action in the case of the failure> (1) Disk array PS OFF/ON, (2) Or dummy-replacing CTLs one by one, (3) Or rebooting CTLs one by one, (4) Or disconnecting/reconnecting			
	V8.8/A, 0888/A							2/22/2010	198	None
V8.8/A 0888/A Base System V8.5/C, 0885/C	1	N	-	-	-	SAS HDD is supported for RKAKX (Dense tray).	SAS HDD is supported for RKAKX (Dense tray). Note: There are restrictions for installing SAS HDDs into Dense tray: (1) SAS HDDs and SATA HDDs must not be coexisted in one Dense tray (SAS HDD and SATA HDD can be distinguished easily because of different canister design.) (2) SAS HDDs must not be installed on the slot #19 to #23 in Dense-A/Dense-B tray (SAS HDDs must be installed on the slot #0 to #18 in Dense-A/Dense-B tray.) (3) Dense Chassis Rev.B and Rev.D (Serial Number is 88010207 or smaller) are NOT available for SAS HDD. The Firmware 0888/A can't detect the illegal configurations for above three restrictions (1) (2) (3). The checking function for (1) (2) is to be supported in the firmware 0890			
	V8.5/D, 0885/D							3/1/2010	199	18
V8.5/D 0885/D Base System V8.5/C, 0885/C	1	I	-	None	-	The DP pool operation time is improved.	The DP pool operation time * is improved. (*: The creation and the capacity expansion of the DP pool)			
	2	I	-	None	-	The preparation time of DP pool optimization is improved.	The preparation time of DP pool optimization is improved.			
	3	C	A	None	V90-0230, V85-0084	Host I/O Performance is down after selecting the "Dynamic Provisioning Optimization" as priority mode in Dynamic Provisioning Optimization.	DF800-EN-M038 [Phenomena] Host I/O Performance is down after selecting the "Dynamic Provisioning Optimization" as priority mode in Dynamic Provisioning Optimization. <Equipment model> DF800H/M/S <Firmware version> V8.0/A(0880/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Dynamic Provisioning is enabled. (2) Selecting "Dynamic Provisioning Optimization" as priority mode in Dynamic Provisioning Optimization. (3) Receiving the Host I/O. [Cause] Firmware bug. When executing the Dynamic Provisioning Optimization with "Dynamic Provisioning Optimization" priority mode, all Host I/Os are not executed by special logic for prioritizing Host I/O, but are executed by normal I/O process. However, causing by the Firmware bug, the I/O process is not returned to execute the special logic for prioritizing Host I/O even though the actual Dynamic Provisioning Optimization process is completed. Therefore, this performance degradation continues until changing the priority mode to "Host Access". <Countermeasure> The Dynamic Provisioning Optimization with "Dynamic Provisioning Optimization" priority mode is not referred by I/O process, when only Dynamic Provisioning Optimization process is not executed. <Action in the case of the failure> Selecting "Dynamic Provisioning Optimization" as priority mode in Dynamic Provisioning Optimization.			

	4	C	A	None	V85-0090, V85-0091	The subsystem down is occurred by illegal Dynamic Provisioning control information when Dynamic Provisioning control information is referred.	[Phenomena] The subsystem down is occurred by illegal Dynamic Provisioning control information when Dynamic Provisioning control information is referred. <Equipment model> DF800H/M/S <Firmware version> V7.0/A(0870/A) to V7.2/G(0872/G) [Conditions of Occurrence] The problem may occur when each following conditions are occurred. (1) Dynamic Provisioning is enabled. (2) Controller failure/Temporary Controller failure/unexpected power off occurs during Dynamic Provisioning pool operation at firmware version 7.0/A to 7.2/G . (3)After upgrading the firmware as online firmware update or [Cause] Firmware bug. When a failure occurs during Dynamic Provisioning pool operations, the control information of Dynamic Provisioning is not generated correctly. If the delete operation for this pool is executed, the control information is not deleted correctly. <Countermeasure> Even though a failure occurs during Dynamic Provisioning pool operations, the control information of Dynamic Provisioning is recovered correctly. <Action in the case of the failure> Please execute power off and on. Then the control information of Dynamic Provisioning is recovered.
	5	C	A	DF800- 26071(SD3021569)	V85-0088, V90-0246	Subsystem down with "Watch-dog time-out" on the both controllers, when upgrading the model	[Phenomena] Subsystem down with "Watch-dog time-out" on the both controllers, when upgrading the model <Equipment model> DF800H/M/S <Firmware version> All Version [Conditions of Occurrence] The problem may occur when each following conditions are occurred. (1) Execute model upgrade. [Cause] Firmware bug. On the model upgrade, it takes longer time than expected to extract the configuration of the array and the trace information from the HDU to the memory on the controller. Thus the firmware detects the timeout (Wathc-dog time-out, 10sec.) for the process. <Countermeasure> Fix the process not to occur the Watch-dog time-out. <Action in the case of the failure> (1) Connect LAN cable to the both controllers of the upper grade model (2) After(1), exectute PS-OFF/ON (3) After (2), set the PageRefreshMode on the management Web screen
	6	C	B	D800- 25096(SD2987824)	V85-0076, V90-0185	When uncorrectable error occurs in a SAS HDU, the HDU is blockaded.	[Phenomena] When uncorrectable error occurs in a block of a SAS HDU and Write operations to the block are executed, the reassignment of the block is not done and the HDU is blockaded with Write failure error. Message: "I41900 HDU error over" <Equipment model> DF800H/M/S, SA8x0 <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when each following conditions are occurred. (1) SAS HDU

							[Cause] Firmware bug. When uncorrectable error occurs in a block of a SAS HDU, the reassignment to the block is executed by the firmware. In some cases, write command (e.g. host I/O, HDD recovery, etc.) is issued to the block before the reassignment is done and write failure response (03/0C03) is sent from the HDU. This write failure is managed by the threshold check of the write failure itself and the HDU will blockaded as results. <Countermeasure> Fix the firmware as follows: As write failure response (03/0C03) is caused by the uncorrectable error, the threshold check of the write failure is managed by the threshold check of the reassignment (instead of the threshold check of the write failure itself.)	
	7	C	B	None	V85-0092	During RAID group expansion, time-out of host I/O and SNM2(set/refer) and CCI (set/refer) , and remote-path failure occurs.	[Phenomena] Time-out of host I/O and SNM2(set/refer) and CCI (set/refer) , and remote-path failure occurs.when RAID group expansion collides with LU exclusion operation(process). The above time-out continues to occur for up to about 10 hours <Equipment model> DF800H/M/S <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when each following conditions are occurred. (1) RAID group expansion is running (2) LU exclusion operation(process) are executed (3)Host commands are executed on LUs when the LUs are the targets of the operation(2)(processes(2)) and RAID group expansion is running on the different controller. Or two RAID group expansions are executed at the same time. List of the operations(2) and processes(2): (a) Receving Mode Select command(0Ah page) (b) Receiving Persistent Reserve Out command (c) Pair Operation(ShadowImage, SnapShot, TrueCopy, TrueCopy Extended Distance(TCE), Moduler Volume Migration) (d) Data Retention Utility Operation (e) Unifying LUs (f) LU ownership switching process. (g) Parity Correction (h) Formatting LU (i) ShadowImage copy process (j) TrueCopy copy process (k) TCE copy process (l) TCE pair process (m) Snapshot restore process [Cause] Firmware bug. There are cases where the LU exclusion operation(process) continues to wait until RAID group expansion which has no relation to the LUs. As a result, time-out occurs in host I/O and SNM2 or CCI commands(set/refer) to the specified LUs. <Countermeasure> The firmware is modified so that the LU exclusion operation(process) does not continue to wait for the completion of the RAID group expansion which has no relation to the LUs. <Action in the case of the failure> In cases that the time-out continues to happen, execute the Power OFF/ON.
	8	C	B	None	V85-0078, V90-0238	Controller blockade on the diagnosis of the start up of the array	[Phenomena] When starting up the array, DCTL hard error[OWN_CTL] is detected by the diagnosis of the hardware and the controller is blockaded. <Equipment model> DF800H <Firmware version> All Versions [Conditions of Occurrence] The problem may occur when each following conditions are occurred. (1) DF800H (2) Start up the subsystem The occurrence depends on the timing of the firmware execution. [Cause] Firmware bug. The exclusion between the acesses among the CPU cores on the diagnosis when the startup of the subsystem is insufficient. Thus the firmware detects the failure on the DCTL wrongly. <Countermeasure> Fix the bug by correcting the access timing exclusion between the accesses among the CPU cores to the same resource. <Action in the case of the failure> Please execute power off and on.

	9	C	C	None	V85-0089	The pool format message of beginning and the end might be not displayed.	[Phenomena] The pool format message of beginning and the end might be not displayed. <Equipment model> DF800H/M/S <Firmware version> First version or later [Conditions of Occurrence] The problem may occur when each following conditions are occurred. (1) Dynamic Provisioning is enabled. (2) While Dynamic Provisioning pool creation or capacity addition operation. (3) Controller failure/Temporary Controller failure/unexpected power off occurs. [Cause] Firmware bug. The controller failure/Temporary Controller failure/unexpected power off occurs while Dynamic Provisioning pool creation / capacity addition operation, failure recovery information might be discarded. <Countermeasure> The controller failure/Temporary Controller failure/unexpected power off occurs while Dynamic Provisioning pool creation / capacity addition operation, failure recovery information might be maintained to the last operation. <Action in the case of the failure> None			
	V9.0/A, 0890/A							3/12/2010	203	None
V9.0/A 0890/A	1	N	-	None	-	New controller support	- New controller supports the following features. LAN 2chip/CTL Onboard FC I/F in RKES/RKEM Multi Protocol (FC/iSCSI) in RKES/RKEM 255HDDs on RKEM with 5 RKAKX			
Base System V8.5/D, 0885/D	2	N	-	None	-	VMware vStorage API for Array Integration (VAAI) support	- Supported Full XCOPY command - Supported Compare and Write command - Supported Write Same command			
	3	N	-	None	-	Enhancement of Dynamic Provisioning	- Maximum capacity is enhanced with 2TB SATA HDDs on RKES/RKEM/RKEH. - Model Upgrade Support Model upgrade with Dynamic Provisioning function is supported.			
	4	N	-	None	-	Year 2010 Compliance	Year 2010 Compliance with NIST Minimum Security Strength			
	5	N	-	None	-	Capture Port Error Count support	Support Capture Port Error Count with using Hitachi Storage Navigator Modular 2 CLI			
	6	N	-	None	-	PGR Key 128 in RKES/RKEM/RKEH for Windows 2008	PGR Key 128 in RKES/RKEM/RKEH for Windows 2008 R2 Cluster Shared Volume configuration.			
	7	N	-	None	-	All capacity quick format with 2TB HDD configuration	Support all capacity quick format with 2TB HDD configuration			
	8	N	-	None	-	Forced Reserve Reset support	Support Forced Reserve Reset with Hitachi Storage Navigator Modular 2 GUI Unintentional LU reservation can be released with using this function.			
	9	N	-	None	-	Enhancement of Performance Monitor	Performance Monitor shows Sequential I/O performance numbers and Random I/O performance numbers.			
	10	I	-	None	-	RAID 1+0 SATA performance	Improvement of SATA performance on RAID 1+0 configuration.			
	11	I	-	None	-	Host I/O response time during DP-Vol	Improvement of Host I/O response time during DP-Vol operation			
	12	I	-	None	-	ShadowImage pair can be created during the DP(Dynamic Provisioning) Optimization	ShadowImage pair can be created during the DP(Dynamic Provisioning) Optimization is running on the pair LUs			
	13	I	-	EUC1053596	-	capturing trace data when Write command response time out (B/C006) occurs	Improvement for the capturing trace data when Write command response time out (B/C006) occurs			
	14	I	-	None	-	DP-Vol Page Garbage collection function	Improvement of DP-Vol Page Garbage collection function			
	15	I	-	None	-	Performance Monitor to display DP Pool	Improvement of Performance Monitor to display DP Pool			
	16	I	-	None	-	Simple Trace information improvement and partitioning of trace file	Simple Trace information improvement and partitioning of trace file			
	17	I	-	None	-	New parameter “Subsystem boots up after the HDD has been removed during subsystem power-off” of the MENU “Others” is supported in the WEB display of the maintenance mode of	Subsystem can boot up after the failure HDD has been removed in the offline of subsystem, if above parameter has been set to "Enable" (default: "Disable (normal boot-up)"), when subsystem cannot boot up due to the HDD failure.			
	18	I	-	None	-	ShadowImage I/O Switching function for DP-Vols.	In ShadowImage I/O Switching function, DP-Vols can be used for a P-VOL or an S-VOL of ShadowImage.			
	19	I	-	None	-	E-mail message on E-mail Alert function.	Improvement of E-mail message on E-mail Alert function.			
	20	I	-	None	-	Improvement of subnet mask check function	The illegal subnet mask value in LAN configuration can de detected with this function.			
	21	I	-	None	-	I/O performance on DP-Vols	Improvement of I/O performance on DP-Vols when setting DP optimization priority mode.			

	22	C	A	None	V90QA037	Subsystem-down for "HF0101 Data transfer check error" during the planned shutdown in DF800H.	[Phenomena] There might be the case of Subsystem-down caused by both CTLs failure for illegally detecting the "Data transfer check error [WRNODTYBK]". <Equipment model> DF800H <Firmware version> V8.5/A(0885/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) DF800H (2) Enabling Copy-on-write Snapshot, ShadowImage in-system replication, TrueCopy remote replication, TrueCopy Modular Distributed, TrueCopy Extended Distance or Dynamoc Provisioning. Or, there are some dirty-data on the Cache. (3) Executing planned shutdown (4) Detecting the CTL failure [Cause] Firmware bug. Regarding the LU Ownership changing process during planned shutdown, it needs to be worked after all job processes completed. However, because of the firmware bug, there is the case to generate new job illegally during the LU Ownership changing process, then it causes the CTL failure in the other side and Subsystem-down at last. <Countermeasure> Modify the logic not to generate new job process in above case. <Action in the case of the failure> Executing planned shutdown and booting again. Then executing the planned shutdown again.
	23	C	A	None	V90-0266	Subsystem-down caused by other side of CTL failure during the DP Pool initializing process.	[Phenomena] There might be the case that Subsystem-down occurs caused by other side of CTL fialure which detects the "HJ4AC7 Microprogram error was detected[HDP]" illegally if CTL failure is occurs during DP Pool initializing process. <Equipment model> DF800S/M/H <Firmware version> V7.0/A(0870/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Enabling Dynamic Provisioning (2) Executing the DP Pool initialization (3) Detecting the CTL failure [Cause] Firmware bug. Logical contradiction is detected when LU ownership changing process refers the intenal table illegally in the case of CTL failure during the DP Pool initializing process. <Countermeasure> Modify the timing to refer the internal table to avoid illegal table access. <Action in the case of the failure>
	24	C	A	None	V90-B001	Subsystem-down caused by route switching (VRRP) of L3 Switch during I/O operation.	[Phenomena] Subsystem-down occurred by the switching (VRRP) of route of L3 Switch while I/O operation. DF800H/M/S, V3.2/A(0832/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)iSCSI I/F (2) Login from 176 or more initiators per a port (3)Execute VRRP switching Firmware bug. Virtual MAC address of passing became invalid in login by the VRRP switching, and the Nop-In command did not end. Therefore, the resource to execute Login processing by retry before the interruption ended repeating retry of the NOP-In command was insufficient, and the controller blockage was occurred. <Countermeasure> The timer was shortened so that the Nop-In command may end, and the resource was not insufficient. <Action in the case of the failure>

	25	C	A	None	V90QA011	Subsystem-down when one controller fails while LUs are formatted or parity correction is executed.	[Phenomena] The subsystem goes down when one controller fails while LUs are formatted or parity correction is executed. The following message is displayed "Resource release time-out was detected[Core]. <Equipment model> DF800H <Firmware version> First Version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)Multi-core configuration installed(DF800H) (2)The configuration information is being changed at the time of the following events (i)The configuration information is being changed when LUs are formatted. (ii)The configuration information is being changed when parity correction is executed. Firmware bug. Resource is obtained to make mutual exclusion between the controllers or the cores when the configuration information for formatting LUs and parity correction is changed. And there are cases where deadlock between the cores may occur in the process of recovering the controller failure and then time-out of resource occurs due to the logic for avoiding the dead-lock. And then the remaining controller comes to fail, which means both of the controllers fail. <Countermeasure> In the logic for avoiding dead-lock, countermeasures to reset the process of obtaining resource are taken so as to prevent the time-out of resource. <Action in the case of the failure>
	26	C	A	None	V90-B004	Subsystem-down occurs when an ENC is pulled out.	[Phenomena] Subsystem down occurs when an ENC which installed in the enclosure with one or more SATA drives is pulled out. DF800H/M/S, First version or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) One or more SATA drives is installed in the system. (2) An ENC which installed in the enclosure with one or more SATA drives is pulled out. The pulled ENC is not blockaded. (This phenomena doesn't occur in case that an ENC which is blockaded is pulled out.) ENC Firmware bug. This phenomena occurs when the ENC is pulled out in the timing of executing SES access from firmware to a pair ENC of pulled out ENC by way of pulled out ENC. The expected behavior of the ENC which was executed SES access from firmware is to finish retrying the response to firmware by two seconds. But the ENC firmware has a bug which is that time out counter is cleared illegally and the tasks in the ENC which was executed SES access continue to execute unexpectedly. So the number of tasks is over the regulation, the ENC is blockaded and subsystem down occurs. <Countermeasure> The countermeasure is by ENC Firmware bundled in firmware. The ENC which was accessed by SES finishes retrying the response to firmware by two seconds (Time out value). <Action in the case of the failure>
	27	C	A	None	V90-0079	Subsystem outage may occur in the power-on after the electriacl power outage.	[Phenomena] (phenomenon-1) When more than one spare disk drive has been replaced in the past, subsystem outage may occur with the following message in the power-on of subsystem after the electrical power outage and cache memory volatilization. WEB information message: "I6G100 The serial number of the HDU is different from the configuration info", "HH9R00 Two or more HDUs have serial number problem" (phenomenon-2) When one spare disk drive has been replaced in the past, the blockade of this drive may occur with the following message in the power-on of subsystem after the electrical power outage and cache memory volatilization. WEB information message: "I6GV00 Move drive (Unit-x1,HDU-y1) to slot (Unit-x2, HDU-y2) because of serial number problem" <Equipment model> DF800H/M/S <Firmware version>

							[Conditions of Occurrence] When all of the following conditions are met, the phenomenon occurs. (a) More than one spare disk drive is replaced. (in case of phenomenon-1) One spare disk drive is replaced. (in case of phenomenon-2) (b) The subsystem configuration information is not updated to the system disk of subsystem after the replacement of (a). (For example, LU creation, system parameter setting, host group option setting and subsystem shutdown etc. are not executed.) (c) The electrical power outage and cache memory volatilization occur under the condition of (b). (d) the power-on of subsystem is executed after the condition of (c). [Cause] Firmware bug. The firmware incorrectly checks out the spare disk drive by using the old subsystem configuration information in the power-on of subsystem after the electrical power outage and cache memory <Countermeasure> The firmware writes the subsystem configuration information to the system drives, when a spare disk drive is replaced. <Action in the case of the failure> Please perform one of following procedures. (a) After a spare disk drive is replaced, please deactivate the spare disk drive setting for this disk drive once, and then reconfigure the spare disk drive setting. (b) Subsystem power-off/on
	28	C	B	None	V90-0260	WEB connection failure on failed CTL in DF800H with iSCSI I/F	[Phenomena] There is the case that the failed CTL cannot be connected by WEB in DF800H with iSCSI I/F. <Equipment model> DF800H, V1.0/A(0810/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) DF800H (2) iSCSI I/F (3) Detecting the CTL failure Firmware bug. Process for CTL failure halts inappropriately for uncorrectable error when one hardware-reset and iSCSI register access occur simlutaneously, then the CTL cannot connected by WEB. <Countermeasure> Removing the unnecessary register access. <Action in the case of the failure>
	29	C	B	None	V90-0061 V90-0089 V90-0175	Controller 0 hung-up when starting the Maintenance Mode	[Phenomena] Letting the subsystem to enter the maintenance mode, the controller 0 does not reply to the Web access and other operations. DF800H/M, V6.0/A(0860/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) The system drives of the subsystem are SAS HDD (2) Let the subsystem to enter the Maintenance Mode (See the Maintenance Manual). Firmware bug. Due to the application of patches to the internal OS were incomplete on V6.0, the firmware may access to the memory whose address is illegal on the SAS HDD access process in the Maintenance Mode. <Countermeasure> Apply all the necessary patches to the internal OS to fix not to access the illegal memory area. <Action in the case of the failure> Dummy replace of the controller (Remove the controller and insert
	30	C	B	None	V90-0114	Unable to access by HSNM2	[Phenomena] When creating a RAID Group made of the maximum number of HDDs of the model, the subsystem can not be accessed from HSNM2. (HSNM2 Message: DMEA001163: The value received from the subsytem is invalid) <Equipment model> DF800H/M/S, All version [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Creating a RAID Group made of the maximum number of HDDs of the model (e.g. 480 for DF800H). The RAID configuration is not RAID1 and not RAID0(2D)

							Firmware bug. The process to get the information of all HDDs in a RAID Group has a bug on the terminate condition to get information. If a RAID Group is made of the maximum number of HDDs of the model, the process fail to terminate and the information to be sent to HSNM2 becomes wrong. <Countermeasure> Fix the process to get the information of all HDDs in a RAID Group. <Action in the case of the failure> None. (As the RAID Group cannot be removed, the clear of the system configuration or the initial setup is necessary.)
	31	C	B	None	V90-0169	Link-up failure during Array booting, CTL recovery process, Firmware upgrading and CTL reset process	[Phenomena] The link-up couldn't do after the boot operation of apparatus(PS-ON, Offline firmware exchange, temporary controller failure). <Equipment model> DF800H/M/S, V3.2/A(0832/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)FC I/F (2)The boot operation of apparatus(PS-ON, Offline firmware exchange, temporary controller failure) (3)The cable is connected. (4)Loop Bypass signal had been accepted before light was output. Firmware bug. When the aparatus is boot, light is output from the AMS side. The Link initialize is executed at the case of the speed fixation. When the FC port accepts the Loop Bypass signal, Link Initialize isn't executed. At this time, when the FC port accepts the Loop Bypass signal, Link Initialize doesn't is executed. <Countermeasure> Retrying can be executed for the start-up of the apparatus. <Action in the case of the failure> The cable is pulled off, and execute the operation of controller's
	32	C	B	None	V90-0191	When the setting change between Enable and Disable for the Switch port, the controller blockage is occurred.	[Phenomena] When Enable/Disable of Switch port is switched, the controller blockage is occurred. <Equipment model> DF800H/M/S, V3.2/A(0832/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)FC I/F (2)The setting of the topology is Point to Point. (3)Switch connection Firmware bug. LS_RJT responds when the LISM frame is accepted at the opportunities other than the link initialization at the Point to Point connection. An internal resource was insufficient because of executing responded for the LISM frame, and the controller was blockaded. <Countermeasure> (1)When the LISM frame is received, the received frame is cancelled. (2)When the ACC for FLOGI is waiting, the received frame is
	33	C	B	None	V90-0228	The controller blockage was occurred by pulling out the cable in the SAN environment except for the path between AMS and Switch.	[Phenomena] The controller blockage was occurred by pulling out the cable about the SAN environment other than AMS-Switch connection. HJ0834 Microprogram error[FSM] <Equipment model> DF800H/M/S, V3.2/A(0832/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)FC I/F (2)Reset is accepted to the number of 4096 or more in AMS2300 and the number of 2048 or more in AMS2100. Firmware bug. Because there was a bug that mistakes the range of reset when the reset command is received. <Countermeasure> When the reset command is received, the command is cancelled at condition of occurrence (2).
	34	C	C	None	V90-0051	WEB connection failure when getting the Simple Trace just after CTL failure	[Phenomena] In DF800H, there might be the case that getting Simple Trace is failed then WEB cannot be connected when the Simple Trace collection is executed on the failed CTL within 3min after CTL failure. <Equipment model> DF800H, V1.0/A(0810/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) DF800H (2) Detecting CTL failure

							Firmware bug. Both CTL failure process and Simple Trace collection process access same area in Flash memory illegally, then both of them cannot use this area. <Countermeasure> Process of Simple Trace collection retrys after 1sec if it cannot use that Flash memory area in above case. <Action in the case of the failure> Moving to WEB Maintenance Mode, then getting the Simple Trace again.
	35	C	C	None	V90-S020	Illegal event log message for I/F Slot#1 in DF800H with multi protocol	[Phenomena] I/F Slot number is shown illegally as #0 even though it is actually for #1 in DF800H with multi protocol. <Equipment model> DF800H, V6.0/A(0860/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) DF800H (2) "CTL0-I/F Slot#1 is iSCSI, and CTL1-I/F Slot#1 is FC" or "CTL0-I/F Slot#1 is FC, and CTL1-I/F Slot#1 is iSCSI" (3) Turnning on the Array Firmware bug. In above case, fixed #0 is shown in every case. <Countermeasure> Fix above logic appropriately. <Action in the case of the failure>
	36	C	C	None	V90-0177	The contents of Audit Log is illegal when installing the Program Products	[Phenomena] When installing/de-installing a Program Product, the Audit Log should be "Start/NotStart" as written in the user's guide, but the Audit Log actually issued is "Enable/Disable". <Equipment model> DF800H/M/S, All version [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Audit Logging is enabled. (2) Installing/De-installing a Program Product. Firmware bug. On the management table for the Audit Log, the correspondence between the event code of the installation of Program Products and the string to be displayed was wrong. <Countermeasure> Fix the correspondence between the code and the string on the table. <Action in the case of the failure> None.
	37	C	C	None	V90-0262	When the PS off is executed, the controller blockage is occurred although the PS off completes.	[Phenomena] When the PS off is executed, the controller blockage is occurred. However, the PS off is completed. <Equipment model> DF800H/M/S, V6.0/A(0860/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)iSCSI I/F (2)AMS2500 Firmware bug. It was a specification that stopped processing when Hard Reset was executed in the core where iSCSI I/F was mounted when the PS off is executed. However, the apparatus could not recognize that the controller blockage processing was executed and controller blockage was occurred. <Countermeasure> Even if Hard Reset is executed, the controller blockage isn't
	38	C	C	None	V90QA020	Illegal message is displayed when ENC cable is connected incorrectly.	[Phenomena] When subsystem is booted up, the cables are connected incorrectly. For example, - Connection A: between controller enclosure and Unit02-ENC0. - Connection B: between controller enclosure and Unit03-ENC0. - Connection A and B are swapped each other. Web massage shows that the connection of Unit02-ENC1 is incorrect instead of Unit02-ENC0. HH7700 Backend down[Cable error](Unit-02,ENC-1) <Equipment model> DF800H/M/S, V3.1/A(0831/A) or later [Conditions of Occurrence] The problem will occur when all following conditions are met. (1) Subsystem boot with illegal cable connected status OR enclosure online addition with illegal cable connected status OR power on about tray power saving with illegal cable connected status

							Firmware bug. There is a bug about consistency detection logic for backend connection, so firmware misjudges that the connection of ENC0 that is checked previously is "correct". <Countermeasure> Web message shows only Unit number. ENC number (0 or 1) isn't shown. <Action in the case of the failure> Power off for all enclosures and please connect the ENC cables about Unit number which is shown by Web message correctly. Then please reboot the subsystem.		
	39	C	C	SD3355357	V90-0061	The connection delay to Web or the connection failure to Web occurs after port scan is done.	[Phenomena] (1) When the connection to Web is tried by http (80 port), the connection delay or the connection failure occurs. (2) When the connection to Web is tried by https (443 port), the connection delay occurs. <Equipment model> DF800H/M/S, V6.0/A(0860/A) or later [Conditions of Occurrence] The problem will occur when all following conditions are met. The connection delay to Web by https (443 port) occurs. (1) The port scan is executed to https (443 port). The connection delay to Web by http (80 port) occurs. (1) The port scan is executed to http(80 port). (2) Https(443 port) is normal. The connection failure to Web by http(80 port) occurs or the connection delay to Web by https (443 port) occurs Firmware bug. WEB uses http (80 port) and https (443 port).In the user environment, when the port scan does the incoming connection to https(443 port), then the connection is reset instantly, WEB becomes the input waiting state to https(443 port). Therefore, it become impossible for WEB to respond to the connection from http(80 port). And the connection delay occurs because https (443 port) or http(80 port) is the input waiting state by port scan too. It is not possible to respond to the connection until becoming an input waiting time-out. <Countermeasure> The port connection processing of WEB is corrected. <Action in the case of the failure> (1) It is connected to Web by https(433 port).		
	V8.5/F, 0885/F							3/24/2010	215 None
V8.5/F 0885/F	1	I	-	D800-81367 (SD3045467)	V85-0096	Detect function against unformatted areas caued by the unexpected termination of LU format	Detect function against unformatted areas caused by the unexpected termination of LU format. This function runs either of the startup/reboot of the subsystem (including firmware update). If an unformatted area is detected, an information message will be issued: "Unformatted area remains in the LU(LU-XXXX)".		
Base System V8.5/D, 0885/D	2	C	A	D800-25136 (SD3006769), DF800-26159 (SD3044706)	V85-0094	The controller blockage is generated when AMS is used by USP_V/VM's Universal Volume Manager function.	[Phenomena] The controller blockage is generated when AMS is used by USP_V/VM's Universal Volume Manager function. <Equipment model> DF800H <Firmware version> DF800H, V4.0/A(0840/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Fibre Channel interface (2)DF800H is used by USP_V/VM's Universal Volume Manager function (3)I/O are executed [Cause] When USP_V/VM's Universal Volume Manager is used, the I/O issues by the Round robin method from USP_V/VM to two or more ports at DF800H. Because half the number of I/O are processed by the controller on the side which have the LU owner, I/O load rises. The hardware trouble is detected wrongly to depend on the access-timing of hardware. <Countermeasure> To decrease the I/O load to the controller without the LU owner, the order of I/O processing is adjusted between LU owner controller or LU nonowner controller. <Action in the case of the failure> Please execute the dummy-replace of blocked controller.		

	3	C	A	DF800-25065 (SD2992903)	V90-0280	The controller blockade is occurred by LA error.	[Phenomena] The controller blockade may occur with the following WEB information message during highly-loaded host I/O. WEB information message: "HD5Exy Host transfer DMA error was detected(CTL-x,DMA-y)" <Equipment model> DF800H/M/S <Firmware version> V3.2/A(0832/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. [Cause] Firmware bug. When the processing that judges the end of the data transfer competes between controller's CPU cores, when the data transfer to the cache memory has not completed, there is a case to misjudge that the end of data transfer. <Countermeasure> The end judgment of the data transfer is executed whenl the data transfer to cache is completed by hardware. <Action in the case of the failure> Please execute the dummy-replace of blocked controller. Please execute PS OFF/ON when the controller blockage is generated at both controllers. In that case, the cache volatilizing is not done, and do not pull out the battery.			
	4	C	B	DF800-54001 (EUC1152783)	V85-0098	The controller blockade is occurred with the message "Resource release time-out"	[Phenomena] The controller blockade is occurred with the message "Resource release time-out" <Equipment model> DF800H/M/S <Firmware version> V7.0/A(0870/A) or later [Conditions of Occurrence] The problem may occur when following conditions are met. (1)Enabling Dynamic Provisioning (2)Capacity of Dynamic Provisioning Pool is large. (more than 120TB / system) (3)Dynamic Provisioning Pool is unused, or 4 or less than DP-Vols per a Dynamic Provisioning Poolare defined or unused DP-Vol exists. The problem may occur when any of the following conditions are met. (4)Every 24 hours (5)CPU boot (PS/ON, Firmware Exchange, Insert the Controller) (6)Shrinking the DP-Vol (7)Dynamic Provisioning Optimization [Cause] Firmware bug. At the case of the occurrence condition (4) to (10), after deleting a assigned page, the full page in chunk might become unused. There is the procedure of garbage collection that checks whether the relation with LU can be released. This processing is regularly done during the constant time. When processing is not completed, it ends once. There is no opportunity when processing is completed on the way for the chunk of non reclaimable.Therefore, it takes time to check chunk when there are a lot of unused areas, and the watch-dog error is generated. <Countermeasure> The procedure of garbage collection ends the check for chunk of non-object within the constant time.			
	V9.0/B, 0890/B							3/31/2010	217	019
V9.0/B 0890/B Base System V9.0/A, 0890/A	1	N	-	None	V90-0236	SAS HDD for RKAKX (Dense tray).	SAS HDD (AKH450X(S1) and AKH600X(S)) are supported for RKAKX (Dense tray).			
	2	I	-	DF800-81367/26167/53984(SD3045467)	V90-0297	Detect function against unformatted areas caused by the unexpected termination of LU format.	This function runs either of the startup/reboot of the subsystem (including firmware update). If an unformatted area is detected, an information message will be issued: "I6H100 Unformatted area remains in the LU(LU-XXXX). Please			
	3	I	-	None	E10-0433	Improvement for initialization the SRAM in ENC in reboot sequence	Method for initializing the SRAM in ENC to fill with zero data completely			
	4	C	A	D800-25136 (SD3006769), DF800-26159 (SD3044706)	V90-0296	The controller blockage is generated when AMS is used by USP_V/VM's Universal Volume Manager function.	[Phenomena] The controller blockage is generated when AMS is used by USP_V/VM's Universal Volume Manager function. H06J00 [DCTL]The unexpected completion was detected[E_IRQ6](CTL-0) <Equipment model / Firmware version> DF800H, V4.0/A(0840/A) or later DF800EH, V9.0/A(0890/A) [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) DF800H/EH (2) Fibre Channel interface (3)DF800H is used by USP_V/VM's Universal Volume Manager function			

							[Cause] Firmware bug. When USP_V/VM's Universal Volume Manager is used, the I/O issues by the Round robin method from USP_V/VM to two or more ports at DF800H. Because half the number of I/O are processed by the controller on the side which have the LU owner, I/O load rises. The hardware trouble is detected wrongly to depend on the access-timing of hardware. <Countermeasure> To decrease the I/O load to the controller without the LU owner, the order of I/O processing is adjusted between LU owner controller or LU nonowner controller. <Action in the case of the failure>
	5	C	A	DF800-25065 (SD2992903)	V90-0280	The controller blockade is occurred by LA error.	[Phenomena] The controller blockade may occur with the following WEB information message during highly-loaded host I/O. WEB information message: "HD5Exy Host transfer DMA error was detected(CTL-x,DMA-y)" <Equipment model / Firmware version> DF800H/M/S, V3.2/A(0832/A) or later DF800EH/EM/ES, V9.0/A(0890/A) [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) High load [Cause] Firmware bug. When the processing that judges the end of the data transfer competes between controller's CPU cores, when the data transfer to the cache memory has not completed, there is a case to misjudge that the end of data transfer. <Countermeasure> The end judgment of the data transfer is executed whenl the data transfer to cache is completed by hardware. <Action in the case of the failure> Please execute the dummy-replace of blocked controller. Please execute PS OFF/ON when the controller blockage is generated at both controllers. In that case, the cache volatilizing is
	6	C	B	-	V90-0267	Countermeasure to a bug where the process of recovering a controller failure does not work when deleting arbitrary RAID groups.	[Phenomena] If PS OFF without cache volatilization is performed or a controller failure occurs when deleting arbitrary RAID groups, there are the cases where the RAID groups are deleted but afterward LUs in a RAID group can not be created. Or there is a possibility that WatchdogTimeout can occur due to infinite loop during LU Ownership changing process. <Equipment model / Firmware version> DF800H/M/S, V3.1/A(0831/A) or later DF800EH/EM/ES, V9.0/A(0890/A) [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)Deleting RAID groups (2)LUs are created in the specified RAID groups. (3)During the RAID group deleting sequence, PS OFF without [Cause] Firmware bug. If a failure occurs during decrementing the number of LUs in the RAID group deletion process, the firmware inappropriately decrement the number of LUs again during the failure recovery process. <Countermeasure> Since this problem occurs due to the fact that the value of 'the number of LUs in the system' is not saved in the area for recovering the controller failure, modify the firmware to save the value in the area and retry the RAID group deleting process during the process of changing the controller failure after the value of 'the number of LUs in the system' is set correctly. <Action in the case of the failure> Delete all the RAID groups again, and then create RAID groups
	7	C	B	-	V90-0275	Performance degradation in sequential write on SATA	[Phenomena] Performance degradation in I/O can be seen when sequential writes are issued to LUs in SATA drives. <Equipment model / Firmware version> DF800H/M/S, V5.0/A(0850/A) or later DF800EH/EM/ES, V9.0/A(0890/A) [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Using SATA drives (2) Sequential writes are issued <Internal condition> (3) There are more than 65 segments to skip the parity generation in each drive having unprocessed middle dirty in the previous

							[Cause] Firmware bug. At DF800 V5.0, the firmware was enhanced so that in the process of searching segments to execute collective writing, if sequential writes are issued to LUs in SATA drives and there is unprocessed middle dirty in the previous stripe, the segments in the next stripe let skip(wait) parity generation. In addition, the maximum number of segments to skip parity generation is set and if the number of skipping exceeds the threshold(65), searching segments in the specified RAID group would be stopped and performed in another drive. However the firmware had problem with calculation of the number of skipping and did not count up the number, so all segments in the drive were searched and the middle collective writing took a long time and used a lot of CPU resources, which resulted in the performance degradation . <Countermeasure> Modify the firmware to refer the data through pointers first and to increment it to calculate the number of skipping correctly.	
	8	C	B	-	V90-270	Countermeasure for Loop State Timeout caused by inappropriate logic in the errata of Fibre Channel protocol chip	[Phenomena] Controller failure occurs with following WEB message caused by data transfer check error in 8Gbps Fibre Channel interface. HD2100 Host transfer DMA error was over the threshold <Equipment model / Firmware version> DF800H/M, V7.2/A(0872/A) or later DF800EH/EM/ES, V9.0/A(0890/A) Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Using the 8Gbps Fibre Channel interface (DF800EH/H/EM/M/ES) (2) Host I/Os which data length are less than 8KB [Cause] Firmware bug. The number of data transfer check error caused by inappropriate errata logic (see note1) in 8Gbps Fibre Channel interface exceeds the 6 which is the shreshold, controller failure occurs. note1: When the Loop State Timeout occurs during transferring two short length data, the firmware inappropriately clear both two data although it should clear just the first transferred data. Causing by this, there is a logic contradiction, then the data transfer check error is detected. <Countermeasure> When detecting the Loop State Timeout, the firmware executes the soft reset for the protocol chip to avoid the data transfer check error.
	9	C	B	-	V90-0268	Controller failure in boot up process in DF800H.	[Phenomena] There might be the case that the controller failure occurs in boot up process in DF800H with following WEB message. H0A500 PCI Configuration access error was detected[Host0_PCI Express core, 0x00004000] <Equipment model / Firmware version> DF800H, V3.1/A(0831/A) or later DF800EH, V9.0/A(0890/A) [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) DF800H/EH (Multi Core configuration) (2) I/F board #0 and #1 are same kind of interface. (eg: I/F#0:iSCSI, I/F#1:iSCSI or IF#0:Fibre Channel, IF#1:Fibre Channel) [Cause] Firmware bug. In the process of hardware reset for both two cores on the same controller in boot up process, caused by the firmware bug for exclusion logic of register access in host interface, the firmware inappropriately releases the reset status although the hardware reset process has not been completed yet. Then, the hardware failure is detected illegally and controller is failed. <Countermeasure> The firmware executes the exclusive access for the register in host interface.
	10	C	B	-	800E-007	Illegal controller failure caused by many Link failures in backend diagnosis in array boot up process.	[Phenomena] The controller failure might occur when many Link failures are detected in backend diagnosis in array boot up process with following WEB message. HH9211 Backend diagnosis time-out was detected[code-11] <Equipment model / Firmware version> DF800H/M/S, V3.1/A(0831/A) or later DF800EH/EM/ES, V9.0/A(0890/A) [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Specific term for about 300ms in backend diagnosis in array boot up process. (2) Many Link failures are detected caused by the failure of drive, ENC or controller

							[Cause] Firmware bug. There is a case that the value of progress for the diagnosis becomes abnormal when a Link failure is detected additionally in backend diagnosis, then the controller failure occurs with timeout of the diagnosis. <Countermeasure> Prioritizing the diagnosis process first in the array boot up process, then after completing the diagnosis process, the firmware executes the Link failure process second. <Action in the case of the failure>	
	11	C	B	DF800-26236 (SD3048951)	V90-0308	Cannot issue the SNMP Trap.	[Phenomena] If the config.txt is set with illegal contents at first after installing the SNMP PP key, then SNMP can never be worked normally although the config.txt is fixed normally. <Equipment model / Firmware version> DF800H/M/S, V8.5/A(0885/A) or later DF800EH/EM/ES, V9.0/A(0890/A) [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Installing the SNMP PP key. (2) The Default Gateway is set. (3) The config.txt is set with illegal contents (see note1) at first after installing the SNMP PP key, and following WEB message is displayed. IB1400 SNMP agent detected the error [Cause] Firmware bug. There is a firmware bug in the process of SNMP task generation for the case of illegal config.txt, the SNMP task cannot be generated normally. Then it is never recovered although the config.txt is fixed normally. <Countermeasure> Executing the initialization of SNMP task generation flag before generating the new SNMP task. <Action in the case of the failure> Set the config.txt with normal contents, then executing the array PS OFF/ON.
	12	C	B	-	V85QA012	Controller failure during executing the high-loaded Write which data length is more than 256KB.	[Phenomena] Controller failure might occur with following WEB message during executing the high-loaded Write which data length is more than 256KB. HD2400 DRR time-out <Equipment model / Firmware version> DF800H/M/S, V3.1/A(0831/A) or later DF800EH/EM/ES, V9.0/A(0890/A) [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Executing the high-loaded Write I/Os. (2) The data length is more than 256KB. [Cause] Firmware bug. There is a firmware bug in the process of parity generation for Host Write data. Cause by the illegal logic, the firmware judges the first access as retry process, then detects the retry failure illegally and failes the controller. <Countermeasure> Fix above illegal logic. <Action in the case of the failure>
	13	C	B	-	V90QA008	SAS HDD failure caused by the path failure between ENC and drive.	[Phenomena] When the path between ENC and drive failes, the HDD might failes with no-response status. <Equipment model / Firmware version> DF800H/M/S, V3.1/A(0831/A) or later DF800EH/EM/ES, V9.0/A(0890/A) [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Using SAS HDD. (2) Path failure occurs between ENC and drive, and "Loss of Sync" is detected. (3) The "Loss of Sync" is recovered within 500ms.

							[Cause] Firmware bug. When detecting the "Loss of Sync", the firmware illegally starts the Linkup watching timer, then judges it as Linkup failure with timeout, and the HDD becomes no-responding status. However, the case that "Loss of Sync" status lasts more than 500ms, the firmware can detect the another failure as "Loss of Sync Timeout", there is no problem at this case. <Countermeasure> Fix the above illegal logic for starting the Linkup watching timer appropriately. Followings are FW with countermeasure. AKF400(S1) : 4C03 -> 5C05 AKH300(S2) : 4C51 -> 5C53 AKH450(S1) : 4C51 -> 5C53 AKH600(S) : 4C51 -> 5C53			
	V9.0/D, 0890/D							4/26/2010	228	020
V9.0/D 0890/D Base System V9.0/B, 0890/B	1	C	A	-	V90QA070	Access Lost may occur when multiple SNMP TRAP events occur on a controller at the same time as another controller blockade.	[Phenomena] When SNMP function is enabling and a controller is blockaded, an access lost may occur on another controller due to hang-up. <Equipment model / Firmware version> DF800H, V9.0/B(0890/B) DF800EH, V9.0/B(0890/B) [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) The firmware version of V9.0/B is used. (2) SNMP function is enabling. (3) SNMP server gets MIB information. (4) A controller is blockaded. (5) 2 or more TRAP events caused by some failures on another controller occur at the same time as (4). [Cause] Firmware bug. In case that SNMP server tries to get MIB information, SNMP Task stack overflow may occur with very low possibility caused by the bug. And then pointer addresses area for TRAP messages are overwritten with illegal data due to the stack overflow. In the result, a controller hangs. The problem may appears when a controller is blockaded and 2 or more TRAP events caused by some failures on another controller at the same time as the controller blockade. <Countermeasure> Expand stack size of SNMP task <Action in the case of the failure> Please shutdown by breaker off of a basic unit, and power up			
	2	C	B	-	V90-0317	Automatic collection of Simple Trace via Hi-Track Monitor may fail.	[Phenomena] Automatic collection of a simple trace via Hi-Track may fail. The problem may occur only when a customer is using Dynamic Provisioning. A collection via Storage Navigator Modular2 and Web tool has no problem. <Equipment model / Firmware version> DF800H/M/S, V9.0/B(0890/B) DF800EH/EM/ES, V9.0/B(0890/B) [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) The firmware version of V9.0/B is used. (2) A customer is using Dynamic Provisioning. (3) Hi-Track monitor is connected. [Cause] Firmware bug. When a customer environment is configured with a combination of new firmware V9.0/B and current Hi-Track Monitor version, which does not support an expanded simple trace collection, no simple trace may be collected via Hi-Track caused by the bug. <Countermeasure> I/F between main firmware and Hi-Track when the simple trace is collected is backed before V9.0. In the combination of a new version, new I/F communicates.			
	V9.0/G, 0890/G							5/21/2010	231	None
V9.0/G 0890/G Base System V9.0/D, 0890/D	1	I	-	-	V90-0322	Improvement for signal of the laser beam at onboard Fibre Channel interface on DF800ES/EM	The parameter to control the output signal of the laser beam from array unit is changed to a proper value.			

	2	C	A	-	V90-0325	In configuration that TrueCopy(TC) P-VOL is cascaded with SnapShot(SS) V-VOL, data inconsistency may occur at S-VOL of TC	[Phenomena] In configuration that TC P-VOL is cascaded with SS V-VOL (SS-TC cascade configuration) and a bandwidth of a remote path is set less than 100Mbps, when TC pair creation or resync pair is performed, even if the pair status becomes paired normally, data inconsistency may occur at the TC S-VOL. This phenomenon cannot be detected by DF800. <Equipment model / Firmware version> DF800S/M/H, V4.3/B(0843/B) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] This problem may occur when TC pair creation or pair resynchronization is performed while all of the following conditions are met. (1) TC P-VOL is cascaded with SS V-VOL. (2) A local array of TC is DF800. (This problem occurs when a remote array of TC is both DF800 and DF700) [Cause] Firmware bug. Data transferred over TC is divided into a small length blocks, 0.5KB to 256KB, depending on a bandwidth of the remote path set by user. (The feature that data is divided into small blocks depending on a bandwidth is implemented on V4.3/B when TC iSCSI is supported.) In configuration that TC P-VOL is cascaded with SS V-VOL, each data transfer job divides data into small length blocks and uses incorrectly an address of first block for second block or later, therefore, the corresponding data becomes corrupt. <Countermeasure> The firmware is modified so that each data transfer job uses the appropriate address of blocks for the second block or later. <Action in the case of the failure>	
	3	C	A	-	V90-0325	HJ2570 Microprogram error[RVD] occurs during TrueCopy(TC) initial copy or resync copy and then subsystem goes down	[Phenomena] HJ2570 Microprogram error[RVD] occurs during TrueCopy(TC) initial copy or resync copy and then subsystem goes down.(This problem does not occur for TCE) <Equipment model / Firmware version> DF800S/M/H, V4.3/B(0843/B) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] This problem may occur when TC pair creation or pair resynchronization is performed while all of the following conditions are met. (1)Stripe size of P-VOL is 64KB.(small stripe) (2) RAID Level of P-VOL is RAID5 or RAID6 and the number of data drives(D) is 3,7,11,15,19,23,or 27. (3) A bandwidth of remote path is 12-99Mbps when copy pace is [Cause] Firmware bug. Data transferred over TC is divided into a small length blocks, 0.5KB to 256KB, depending on a bandwidth of the remote path set by user. (The feature that data is divided into small blocks depending on a bandwidth is implemented on V4.3/B when TC iSCSI is supported.) In cases that 192KB is allocated to a job and the transfer length is set to 128KB, the job tries to transfer data which crosses the next stripe line incorrectly, so Microprogram error[RVD] occurs causing controller failures and then the subsystem down. <Countermeasure> The firmware is modified so that job does not transfer data which crosses the next stripe line. <Action in the case of the failure> Disconnect both of the remote path cables and reboot the subsystem. After the reboot, execute the following steps((1)-(2)) and then perform pair resync.(The corresponding pairs become PSUE after reboot)	
	4	C	A	-	V93-S006, V90-0324	The controller blockade is occurred during RG expansion by parity generation LA error.	[Phenomena] Controller failure occurs with following WEB message during expanding RG at DF800EH/EM/ES and same error occurs on the other controller continuously. So, RG expansion does not progress and server connection losts in the top LU of RG. W0N000 Parity generation LA error[DRR](CTL-x) <Equipment model / Firmware version> DF800EH/EM/ES, V9.0/A(0890/A) [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) DF800EH/EM/ES (2) RAID6 (3) Expanding the RAID Group to more than 9 data disk drives	

							[Cause] Firmware bug. A new function to increase data reliability was supported at firmware version 9.0/A on data transfer LSI of DF800EH/EM/ES hardware. DF800E firmware has a bug which set abnormal parameter for data reliability check to LSI (*1), so LSI detects LA error wrongly by calculating the LA value of the RAID 6 Q parity data wrongly. (*1) Originally firmware must set the parameter after expanding the RG, but has set it before expanding wrongly. <Countermeasure> Firmware modifies to set the correct parameter to LSI after expanding RG to calculate the new RAID6's Q parity data. <Action in the case of the failure> (1) Push reset SW of both controllers for changing to maintenance mode. (2) Performe offline microcode exchange to 0890/G and later.		
	V9.0/H, 0890/H								6/23/2010	233	021
V9.0/H 0890/H Base System V9.0/G, 0890/G	1	I	-	-	-	Port-option: Command Unique Response Mode is added.	Port-option: Command Unique Response Mode is added. (Set this option when it takes time for the command to respond)			
	2	C	A	-	V90-0338, V90-B006	After deleting the data pool for S-VOLs of TrueCopy Extended Distance (TCED), the subsystem goes down or the pairs become in error status like PSUE or PFUS.	[Phenomena] After deleting the data pool for S-VOLs of TrueCopy Extended Distance(TCED), the subsystem goes down or the pairs become in error status like PSUE or PFUS. With some of the messages shown below, both of the controllers fail and the subsystem goes down . In cases where the subsystem goes down and trying to reboot still the subsystem goes down, PS OFF with cache volitilization needs to be executed. In that case, data on the cache memory that has not been written to drives will be erased. Messages which can be shown when subsystem down occurs: HJ2CQV Microprogram error[POM] HJ11XX Microprogram error[RCH] HJ12XX Microprogram error[RAD] HJ14XX Microprogram error[DMA] HZ0N0X Kernel processing error(CTL-X) Messages which can be shown when pairs become in error status: IB1S00 PSUE occurred[SnapShot](Data pool-XX) IB1G00 Pair status changed by the error(CTG-X) <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) TCED is enabled. [Cause] Firmware bug. Deleting a data pool needs to be prohibited when TCED pairs exist but such logic is not implemented for the case where the data pool is used only by TCED S-VOLs. After the data pool is deleted, the subsystem may go down or the pairs become in error status. <Countermeasure> A logic is modified to prohibit deleting a data pool even when TCED S-VOLs use the data pool. <Action in the case of the failure> (1) After releasing TCED pairs belonging to the deleted data pool, make a data pool and then create pairs again. (2) In cases where the subsystem goes down and trying to reboot		
	3	C	A	-	V90-0336, V93-0048	In configuration that TrueCopy (TC) P-VOL is cascaded with SnapShot (SS) V-VOL, after deleting V-VOLs, a controller failure occurs and the subsystem goes down.	[Phenomena] In configuration that TrueCopy(TC) P-VOL is cascaded with SnapShot(SS) V-VOL, after deleting V-VOLs, controller failure occurs and the subsystem goes down. When one controller fails, the message "H90210 CTL failure" is displayed on the other controller (A specific factor for this failure is not displayed because this is an exception handing.). When the subsystem goes down after one controller failure, an additional message is not displayed. <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) SS and TC are enabled. (2) After creating a SS pair, a TC pair is created using the SS V-VOL as the TC P-VOL. (3) Deleting the SS pair (The TC pair status becomes PSUE).		

							[Cause] Firmware bug. In a SS-TC cascade configuration, deleting a V-VOL needs to be prevented even when a SS pair is released because the V-VOL still works as TC P-VOL but such a logic is not implemented. Referring to TC pair status after a V-VOL of SS is deleted, differential data is divided by the amount of a LU to get synchronization rate. In this case, the amount of an LU becomes 0, which means differential data would be divided by 0 causing a controller failure. When both of the controllers fail referring to TC pair status, the subsystem goes down. <Countermeasure> The condition for deleting V-VOLs is modified. <Action in the case of the failure> Recover a failed controller(After waiting for the array to be ready following reboot in the case of subsystem down) and then create a
	4	C	A	-	V90-0334, V93-0010	When you use the vStorage feature with failed HDDs, Microprogram error[JSD](HJ3446) occurs causing a controller failure.	[Phenomena] When you use the vStorage feature with failed HDDs, Microprogram error[JSD](HJ3446) occurs causing a controller failure. When both of the controllers fail, the subsystem goes down. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.0/A(0890/A) [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) A problem to cause correction read occurs during staging from drives. (E.g. drive failures or errors) (2) A vStorage command, "Automatically test and set disk block
							[Cause] Firmware bug. While staging from drives is performed if an ATS command is received but cache hit does not happen, correction read is executed for failed drives. At this point, cache memory is released incorrectly, then logical contradiction occurs in subsequent processes and then a controller fails due to Microprogram error[JSD](HJ3446). If both of the controllers fail, the subsystem goes down. <Countermeasure> A logic is modified to release cache memory when receiving ATS commands. <Action in the case of the failure> In the case of a controller failure, replace the controller with a new
	5	C	A	-	V90-0331, V85-0100	I/O timeout of FC port occurs by ACK response waiting of iSCSI port.	[Phenomena] I/O timeout of FC port occurs by ACK response waiting of iSCSI port. <Equipment model / Firmware version> DF800ES/EM/EH, V9.0/A(0890/A) DF800H, V4.0/A(0840/A) [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) DF800H/ES/EM/EH (2) iSCSI/FC Multiprotocol (3) I/O timeout of FC port occurs. [Cause] Firmware bug. The ACK waiting time in the iSCSI port was long, and it was impossible to operate the FC port. Host's application terminated abnormally. <Countermeasure> When the time-out is generated by shortening the timeout period at 3sec, the influence given to other ports is minimized. <Action in the case of the failure> If the storage device is not recognized from the host, device recognition by host (e. g. reboot) is necessary. If some error is occurred on the host application, please retry the operation on the application.
	6	C	A	-	V90-0327, V93-0044	After LIP is accepted, the link initialization terminated abnormally.	[Phenomena] After LIP is accepted, the link initialization terminated abnormally. <Equipment model / Firmware version> DF800EH/EM/ES, V9.0/A(0890/A) DF800M/S, V3.2/A(0832/A), DF800H, V4.0/A(0840/A), [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) DF800EH/EM/ES/H/M/S (2) Fibre Channel interface (3) LIP (Loop Initialization Primitive sequence) accept

							[Cause] Firmware bug. It is set to control the link initialization event to the interface controller chip if the light signal is not accepted during the the Auto Negotiation processing. Because there is no opportunity when the setting of this chip is released if the light signal is accepted during the Auto Negotiation processing, link up becomes impossible <Countermeasure> When the light signal is not accepted during the the Auto Negotiation processing, the disable mode of event report is released. <Action in the case of the failure> (1) Executing planned shutdown and PS-on (2) The controller's dummy exchange	
	7	C	A	-	HDS-0103	After the Dynamic Provisioning pool is deleted, the subsystem down is occurred by the Dynamic Provisioning-Volume deletion.	[Phenomena#1] After the Dynamic Provisioning pool is deleted, the subsystem down is occurred by the Dynamic Provisioning-Volume deletion. HJ4AAK Microprogram error was detected[HDP] [Phenomena#2]After the subsystem down is occurred by the Dynamic Provisioning-Volume deletion, the control information of Dynamic Provisioning is illegal. <Equipment model / Firmware version> DF800H/M(H/W version 0200), V9.0/A(0880/A) [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Dynamic Provisioning is used (2) The firmware version is from 0880/A to 0890/G. (3) DF800M with Hardware version 0200 or DF800H (4) All capacity of Dynamic Provisioning Pools are defined more than 64TB(DF800M (H/W version 0200)) and 192TB(DF800H). (5) One of (5-1)(5-2)(5-3) is executed: (5-1) Dynamic Provisioning pool is deleted. (5-2) Executing planned shutdown and PS-on is executed when the Dynamic Provisioning pool is defined. (5-3) Unexpected power off occurs and PS-on is executed. (6) After (5), the page assigned Dynamic Provisioning-Volumes [Cause] There is a bug in the calculation of the address when the control information of Dynamic Provisioning is saved. Therefore, after the Dynamic Provisioning pool is deleted, the table for the Dynamic Provisioning exclusion has been renewed. The controller blockage was occurred because an unjustified value was stored and this table was referred when deleting Dynamic Provisioning-Volume and formatting it. <Countermeasure> The calculation of the address for the save of the control information of Dynamic Provisioning is modified. <Action in the case of the failure> Please execute either operation. (1) Turn off the power switch of apparatus and PS-on. [case of the subsystem down is occurred by the Dynamic Provisioning-Volume deletion.] (2) Backup the data and execute an initial setup. [case of the subsystem down is occurred by the Dynamic Provisioning-Volume format]	
	8	C	A	-	HDS-0103	The maintenance operation is not completed for Dynamic Provisioning configuration.	[Phenomena] The maintenance operation(HDD recovery, Online parity recovery and Online verify) is not completed for Dynamic Provisioning configuration. <Equipment model / Firmware version> DF800H/EM, V9.0/A(0880/A) [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)Dynamic Provisioning is used (2)The firmware version is from 0880/A to 0890/G. (3)DF800H or DF800M(H/W version 0200) (4)All capacity of Dynamic Provisioning Pools are defined more than 64TB(DF800M (H/W version 0200)) and 192TB(DF800). (5) One of (5-1)(5-2)(5-3) is executed: (5-1) Dynamic Provisioning pool is deleted. (5-2) Executing planned shutdown and PS-on is executed when the Dynamic Provisioning pool is defined. (5-3) Unexpected power off occurs and PS-on is executed. (6) After (5), one of (6-1)(6-2)(6-3) is executed: (6-1) HDD recovery (6-2) Online parity recovery	

							[Cause] Firmware bug. There is a bug in the calculation of the address when the control information of Dynamic Provisioning is saved. Therefore, the Dynamic Provisioning pool is deleted, the table for the Dynamic Provisioning exclusion has been renewed. To get exclusion of resource fails because of the maintenance operation to refer to this table and operation is not completed. <Countermeasure> The calculation of the address for the save of the control information of Dynamic Provisioning is modified. <Action in the case of the failure> Please execute either operation. A. Turn off the power switch of apparatus and PS-on.
	9	C	A	-	V90QA075	Host I/O error and/or the halt of RAID Group Expansion progress	[Phenomena] Host I/O error occurs and/or the progress of RAID Group Expansion progress halts. <Equipment model / Firmware version> DF800H, V8.0/A(0880/A) or later DF800EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) DF800H or DF800EH (2) Exhaust of cache segments (E.g. heavy host I/O load to SATA HDD with lower cache capacity configuration will cause the exhaust of cache segment.) (3) One of (3-1),(3-2) or (3-3): (3-1) RAID Group Expansion (3-2) All of (3-2-1),(3-2-2) and (3-2-3) are met: (3-2-1) Cache segment size is 8KB and stripe size is 256 KB. (Note: This is not the default settings.) (3-2-2) 28D+2P RAID Group configuration, (3-2-3) Paircreate of ShadowImage, pairresync of ShadowImage or the Write command to the LU of PSUS(SP) status in (3-2-2). (3-3) All of (3-3-1),(3-3-2) and (3-3-3) are met: (3-2-1) "Cache segment size is 8KB and stripe size is 256 KB" or "Cache segment size is 16KB and stripe size is 512 KB." (Note: They are not the default settings.) (3-2-2) 28D+2P RAID Group configuration, [Cause] The countermeasure of "Reduction of CPU utilization when the load of I/O is very high."at V8.0/A (ECN DF800-154 Appendix-A rev.2 item 5) has a bug such that if more than 1000 cache segments are necessary to be get at a time, the cache segment exhaust will occur. In the configuration in the Condition of Occurrence, RAID Group expansion needs lots of cache segment (max number is nearly 4000), the RAID Group Expansion progress will be halt. <Countermeasure> Keep the amount of the free cache segment more than 5,000 by periodical monitoring <Action in the case of the failure>
	10	C	B	-	V90-0319 (same as DF700-0280)	When an HDD failure with a terrible vibration occurs, the other HDDs in the same unit may fail caused by the vibration.	[Phenomena] When an HDD failure with a terrible vibration occurs, the failed HDD triggers other HDD failure by the vibration. <Equipment model / Firmware version> DF800S/M/H, All versions. DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] HDD failure with a terrible vibration occurs. [Cause] Due to HDD failure with a terrible vibration <Countermeasure> When an HDU blockade occurs, the new firmware tries the spin down for the failed HDD. <Action in the case of the failure> Please isolate the HDU with the terrible vibration. An then replace the HDU to spare part. Please performe dummy-replavement for the other HDUs.
	11	C	B	-	V90-0327, V93-0044	The command-timeout is occurred.	[Phenomena] The command-timeout is occurred. <Equipment model / Firmware version> DF800H, V4.0/A(0840/A) or later DF800EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) DF800H/EH (2)The interface controller chip detects the Error Idle acceptance. (The Idle signal of the Fibre Channel link cannot be recognized)

							[Cause] Firmware bug. In DF800H/EH, the firmware operates by dual core CPU. The interface control chip is stopped by the Error Idle without the Link failure, and the core that controls interface controller chip is released freeze status. The status doesn't reply to the host even if status is transmitted in cores other than the owner core, there is no processing that resumes the freeze of the chip. Therefore, the command received by other than the owner core becomes the time-out. <Countermeasure> The method of resume the freeze of the interface control chip after Error Idle is accepted is modified. <Action in the case of the failure> None. (ABTS will be transmitted by the host as a result of the
	12	C	B	-	V90-0330	Using a DP-VOL, a temporary error occurs relating to an Extended COPY(XCOPY) whose source and destination are within an identical LU	[Phenomena] Using a DP-VOL, a temporary error occurs relating to an XCOPY whose source and destination are within an identical LU. Even though an error log is left on the server, retrying completes the XCOPY command successfully. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.0/A(0890/A) [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) The source and destination of an XCOPY command are within an identical LU and it's a DP-VOL. (2) Read/Write jobs work within the area of the source and
							[Cause] Firmware bug. If the destination/source of an XCOPY are within an identical LU which is a DP-VOL, there are cases where extent lock does not work because extent lock is not obtained correctly. In that case, extent lock between XCOPY and Read/Write commands does not work and then time-out occurs causing an error. <Countermeasure> A logic of extent log is modified for the case where the source and destination of a XCOPY command are within an identical LU which is a DP-VOL. <Action in the case of the failure>
	13	C	B	-	V90-0333	The controller blockade is occurred at the iSCSI port according to a threshold over of ECC error.	[Phenomena] The controller blockade is occurred at the iSCSI port according to a threshold over of ECC error. HHA400 H-IPC ECC error was detected(CTL-X,I/F-X) <Equipment model / Firmware version> DF800S/M/H, All versions, DF800ES/EM/EH, V9.0/A(0890/A) [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) iSCSI interface (2) ECC errors are occurred at iSCSI port. [Cause] Firmware bug. The statistical information of the iSCSI protocol control chip is acquired in the period 10min, the controller blockades is occurred when it is over threshold (512 or more) of ECC error correction count. The endian conversion is executed by mistake of processing to acquire statistical information. The count actually determines the misjudgment when it is more than threshold (512) in case of count 1, and the controller blockade is occurred. <Countermeasure> The processing of the conversion endian is modified. <Action in the case of the failure> Please pull off and put on the iSCSI interface board (i.e. dummy replace). If the phenomenon reoccurs, please exchange the iSCSI
	14	C	B	-	V90-0328, V93-0047	Unable to detect the correctable error in the cache package #1 during online cache verification	[Phenomena] Unable to detect the correctable error in the cache package #1 during online cache verification <Equipment model / Firmware version> DF800M, V7.2/A(0872/A) or later DF800EM, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) DF800M/EM (2) Two cache memory packages are installed in each controller. (3) A correctable error occurs in the cache package #1. Online cache verification function does not detect the error though that tests the address of (3).

							[Cause] Firmware bug. Online cache verification function of DF800M/EM has a bug such that the function does not count up the occurrence of the error in the cache package #1, though the function counts up the occurrence of the error in the of cache package #0. <Countermeasure> Add the logic to count up the error in the cache package #1 to the DF800M/EM firmware. <Action in the case of the failure> None			
	15	C	A	-	V90-0337	Performance may drop in sequential Read/Write mixture of great length in DF800H/EH temporarily.	[Phenomena] Performance may drop in sequential Read/Write mixture of great length in DF800H/EH temporarily. Messages which can be shown in TDCONV4 when this problem occurs: [1Board array] Detected DRR time-out first time <Equipment model / Firmware version> DF800H, V4.0/A(0840/A) or later DF800EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) DF800H/EH (2) RAID5/RAID6 (3) A segment locked in large quantities (more than 10,000) of a [Cause] Firmware bug. When Firmware shared a segment in both cores in the case of DF800H/EH and got a segment, Firmware searched the segment which Firmware could get.Therefore CPU overheads increased, and performance dropped. <Countermeasure> Firmware starts queue search from the first continuance. <Action in the case of the failure> Please reduce I/O load.			
	V9.3/A, 0893/A							7/21/2010	239	None
V9.3/A 0893/A Base System V9.0/H, 0890/H	1	N	-	-	V93-0002	Dynamic Provisioning with Copy-on-write Snapshot, TrueCopy remote replication and TrueCopy Extended Distance.	Dynamic Provisioning Volume can be used as the volume for Copy-on-write Snapshot, TrueCopy remote replication and TrueCopy Extended Distance.			
	2	N	-	-	V93-0008	VMware vStorage (Xcopy / WriteSame) with ShadowImage in-system replication, Modular Volume Migration, Copy-on-write Snapshot, TrueCopy remote replication and TrueCopy Extended Distance Supporting the vStorage commands in Replication volumes.	VMware vStorage (Xcopy / WriteSame) with ShadowImage in-system replication, Modular Volume Migration, Copy-on-write Snapshot, TrueCopy remote replication and TrueCopy Extended Distance Supporting the vStorage commands in Replication volumes.			
	3	N	-	-	V93-0079	Replication Option enhancement.	Remote Replication Write Control Mode is supported.			
	4	I	-	-	V93-0031	Improve RAID Group and Dynamic Provisioning Pool status.	Improve RAID Group and Dynamic Provisioning Pool status when reconstruction event is underway.			
	5	I	-	-	V93-0011	Improvement for guarding logic of Depletion Alert at Dynamic Provisioning.	Removing current some guarding logic in Depletion Alert with the warning messages.			
	6	I	-	-	V93-0086	Improvement to use back end SAS I/F log (Phy Error Log)information at backend diagnosis.	The function to display a candidate of failure parts on TDCONV4 by getting the Phy Error Log information when array unit can not distinguish an obstacle part by backend diagnosis.			
	7	I	-	-	V93-0131	The improvement of the Drive Response Diagnosis function in RAID1+0 The following check condition is added in order to improve the detection accuracy of the Drive Response Diagnosis function.	The difference in the response performance between the data (or mirror) HDDs in the same backend path. HDS Case#: SD2839381 (same as ECN DF700-391)			
	8	I	-	SD3163287	V93-0153	Improvement of response delay of host command when hard errors occur on disk drives.	Improvement of response delay of host command when hard errors occur on disk drives.			
	9	I	-	-	V93-0003	Improvement to reduce the time for changing IP address.	Improvement to reduce the time for changing IP address online during extremely heavy security attack on the LAN port.			

	10	C	A	-	V93-0143	Countermeasure to the problem that the gurard logic for TrueCopy(TC) operations does not work properly in the configuration where a TC pair is cascaded from a SnapShot(SS) pair	[Phenomena] In the configuration where TC S-VOL is cascaded from SS P-VOL, there are cases where TC operations are not improperly guarded during SS restore. one of the following phenomena occur. (A) In the configuration where TC S-VOL is SS P-VOL, TC re-synchronization and SS restore are being executed at the same time, which makes data of TC S-VOL incorrect. (B) In the configuration where the original P-VOL of TC is SS P-VOL, TC SWAP and SS restore are being executed at the same time, which makes the original P-VOL(new S-VOL) incorrect. (C) Can not execute TC pair operations (pair criate, pair resync, pair swap). <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) TC is used for DF800-DF800 configuration (2) LUs which are moved by Modular Volume Migration(MVM) exist. Or LUs whose LUN is 3996 or later exist when Dynamic Provisioning(DP) is enabled (3) The LUs shown in (2) exist on the remote array (a) A TC operation is performed the remote LU is being restored (Phenomenon (A) or (B) occurs) [Cause] Firmware bug. There is a problem with the process of obtaining SI or SS pair status when the management numbers of LUs within the array are being switched by MVM or HDP. This problem causes TC operations to be guarded improperly. <Countermeasure> The firmware is modified so that LU numbers after switch are used in obtaining SI or SS pair status. <Action in the case of the failure> In the case of Phenomenon (A) or (B), perform the following procedure. (1) Delete the TC pair (2) If the data of TC is needed, create the TC pair again. (If the data of SS is needed, recover the data from backup if possible)
	11	C	A	-	V93-0163	A controller failure occurs or the subsystem goes down with Microprogram error[LSM] message when unsupported port numbers are specified in setting up remote paths from DF800 to DF700	[Phenomena] When an unsupported port number for the DF700 is specified to the remote path for a DF800-DF700 configuration where the DF700 is a remote array, the DF800 controller for the remote path fails with HJ0914 Microprogram error[LSM] message. Setting up both of the remote paths with unsupported port numbers causes both of the controllers to fail and the subsystem goes down on the DF800. Even if PS OFF/ON is performed, the subsystem still goes down every time with Microprogram error[LSM] and can not recover. (PS OFF with cache volatilization can not even recover the subsystem) <Equipment model / Firmware version> DF800S/M/H, V9.0/A(0890/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) TrueCopy(TC)/TrueCopy Extended Distance is enabled (2) The remote path is set up on Fibre channel(FC) (3) DF800 series including DF800E is a local array, and DF700 is a remote array. (4) An unsupported port number for DF700 is specified in remote path settings of port numbers on the DF700. Refer to the table below for unsupported port numbers for DF700 DF700 models　Port numbers which causes problem　Supported ones (Unsupported port numbers)　(For reference) [Cause] Firmware bug. When an unsupported port number is specified on the DF700 in setting up a remote path, the controller fails because there is a problem with the process of checking port numbers on the remote array during remote path setup. When a guard of an unsupported port number for DF800 was changed at DF800E support, a guard of an unsupported port number for DF700 was changed by mistake. <Countermeasure> The firmware is modified so that a controller failure does not occur even if an unsupported port number is specified. <Action in the case of the failure> (1) When a controller fails Delete the remote path. After that, recover the failed controller and then set up a remote path using a supported port number for the remote DF700. (2) When the subsystem goes down Perform offline firmware replacement. When the subsystem is

	12	C	A	-	V93QA041	Countermeasure to the problem that the subsystem goes down with Microprogram error[RVM] when re-synchronization and swap operation are executed at the same time on TrueCopy Extended Distance(TCED).	[Phenomena] Microprogram error[RVM] occurs on both of the controllers of the local array causing subsystem down when re-synchronization on the local array and swap operation on the remote array are executed on TCED pairs in a Consistency Group(CTG) at the same time. Even if you try to recover the subsystem, the subsystem goes down again. <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) TCED pairs exist (2) A pair volume whose pair status is COPY exists in a CTG on the local array. (3) The pair status in the same CTG on the remote array is either PAIR, PSUS, SSWS, or PFUS (Swap operation can be performed on pairs in these status) [Cause] Firmware bug. In the process of checking COPY status of pairs on the local array during swap operation for TCED, it is not determined whether the COPY status came from re-synchronization or swap operation. Therefore in cases where the pair status is COPY by re-synchronization of the P-VOL on the local array to the S-VOL, swap operation can be improperly performed, which causes subsystem down. <Countermeasure> The process of checking the status and attribute of pairs on the local array is modified so that swap operation can not be performed on pair in COPY status on the local array <Action in the case of the failure> Perform (1) or (2)
	13	C	A	-	V93-0134	Countermeasure to the problem that swap operation is not guarded in the configuration where a TrueCopy Extended Distance(TCED) pair is cascaded from a SnapShot(SS) pair	[Phenomena] In the configuration where TCED P-VOL is cascaded from SS P-VOL, swap operation can be perform improperly from S-VOL to P-VOL even when SS P-VOL is being restored and this causes data inconsistency. <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) TCED and SS are enabled. (2) Multiple TCED pairs exist in a Consistency Group(CTG) (3) TCED P-VOL is cascaded from SS P-VOL (4) SS P-VOL is being restored [Cause] Firmware bug. TCED swap operation is not guarded even when SS P-VOL is being restored. <Countermeasure> The firmware is modified so that it guards TCED swap operation when SS P-VOL is being restored. <Action in the case of the failure> (1) The data of SS can not be recovered because correct data of SS P-VOL and V-VOL are not available. Because only the data of TCED P-VOL(the original S-VOL) is correct, if you recover the data of TCED, delete the TCED pair and create a TCED pair using the original S-VOL as the new P-VOL.
	14	C	A	-	V93-0146	Countermeasure for the operation halt and no-response of Host I/O when executing the RG Expansion.	[Phenomena] When executing the RG Expansion, the expansion operation halts and the Host I/O for related LUs cannot be responded. <Equipment model / Firmware version> DF800M/H, V5.2/A(0852/A) or later DF800EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) DF800M/H/EM/EH (2) One of following PPs are enabled, TrueCopy Extended Distance, SnapShot and Dynamic Provisioning. (3) Enabling the CPM, then setting the partition size as below. - less than 480MB for DF800H/EH. - less than 280MB for DF800M/EM. (4) Executing the RG Expansion for RAID6 RG with following use cases. - Expanding from 20 data disks to 21~28 data disks for DF800H/EH.

							[Cause] Firmware bug. There is the firmware bug for the transaction around releasing and reassigning the cache area at the case when enough usable cache space is not remaining. Therefore, the executing RG Expansion does not proceed any more, and the Host I/O for related LUs cannot be responded because it cannot assign enough cache area for the Host I/O process. <Countermeasure> Modifying current inappropriate logic around releasing and reassigning the cache area. <Action in the case of the failure> Apply the fixed firmware by offline firmware upgrading
	15	C	B	EUC1186599	V93-0161	Countermeasure for controller failure when SNMP config setting.	[Phenomena] CTL failure occurs for a cause in Kernel processing error or Watch-dog time-out at the time of SNMP setting. CTL recovery fails if CTL is exchanged. <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) SNMP function enabled. (2) CTL0's or CTL1's IP address is set as SNMP Manager's IP address in CONFIG.TXT(*) file. (3)161 is set as a trap target- (trap to be reported-) port number in CONFIG.TXT. (4) CONFIG.TXT including the setting (1) and (2) above is read out.
	16	C	B	-	V93-0154	Countermeasure for inappropriate controller failure with data check code error when executing the drive read.	[Cause] Firmware bug. Because CTL0's or CTL1's IP address is set as SNMP Manager's IP address, SNMP come to send authenticationFailure Trap endlessly. <Countermeasure> (1) At the time of SNMP setting, it is bacame SNMP configuration error if CTL0's or CTL1's IP address is set as SNMP Manager's IP address. (2) It is limited to send authenticationFailure Trap endlessly. <Action in the case of the failure> (1) Go to maintenance mode. (2) Set a temporary IP address to CTL via Web maintenace mode. (3) Restart the subsystem.
	17	C	B	-	V93-0039	Countermeasure to the problem that pair names are not checked for duplication in creating a remote pair or renaming a pair	[Phenomena] There are cases where remote pairs can be improperly created with an identical name or a pair can be improperly renamed to an already used pair name. Therefore pair operations can not be performed on those pairs. <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) TrueCopy(TC) or TrueCopy Extended Distance(TCED) is enabled (2) Multiple pairs exist in a Consistency Group(CTG) and P-VOLs and S-VOLs exist in the same array. Or Multiple pairs

							[Cause] Firmware bug. Pairs with different pair attribute(P-VOL/S-VOL) are not included in the process of checking pair names for duplication at the time of renaming. <Countermeasure> The firmware is modified so that pairs with different pair attribute(P-VOL/S-VOL) are checked for duplication. <Action in the case of the failure> Rename pairs whose names are overlapped by specifying LU	
	18	C	B	-	V93QA029	Countermeasure to the problem of not completely checking the LUN of an S-VOL during pair creation of TrueCopy(TC) or TrueCopy Extended Distance(TCED)	[Phenomena] The remote path fails when pair creation of TC / TCE is performed. If pairs in COPY or PAIR exist at the time of remote path failure, those pairs also become in PSUE status. <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) TC / TCE are enabled (2) The remote path is in normal status (3) an unsupported LUN (*1) is specified to an S-VOL on Hitachi Storage Navigator Modular2(HSNM2). (*1)LUN of remote array unit. ・DF700S/XS:512 or bigger ・DF700M/DF800S/ES/EXS:2048 or bigger [Cause] Firmware bug. In cases where an unspported LUN is specified to an S-VOL at the time of TC pair creation, because an LUN is not checked during pair creation to determine whether it is supported or not, retries of pair creation are repeated on the local array causing the remote path to fail. <Countermeasure> The firmware is modified so that LUNs are checked during pair creation to determine whether they are supported or not and even if they are unsupported the remote path does not become failed while Check Response is received. <Action in the case of the failure> (1) Recover the remote path on HSNM2	
	19	C	B	-	V93-0099	Countermeasure for inappropriate controller failure when getting the Simple Trace or CTL Alarm Trace.	[Phenomena] The controller failure may occur inappropriately with Watch-dog time-out when getting the Simple Trace or CTL Alarm Trace. <Equipment model / Firmware version> DF800S/M/H, V5.2/A(0852/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) LAN environment is high work-loaded. (File transferring from Array takes more than 10 sec.) (2) Getting the Simple Trace or CTL Alarm Trace. [Cause] Firmware bug. There may be the case that the Host I/O transaction must be waited until time out value because the trace file downloading is prioritized. <Countermeasure> Modifying the logic to allow the other transaction to work periodically to avoid the Watch-dog time-out during the trace file downloading. <Action in the case of the failure>	
	20	C	B	-	V90-S027	ENC blockade when ENC firmware download	[Phenomena] ENC blockade occurs for ENC firmware dowload fail. <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)ENC cable failure (2)Any condition shown below. 1)Microprogram upgrade 2)ENC firmware download 3)CTL exchange	

							[Cause] Firmware bug. There is a bug in ENC firmware download retry logic. And the bug triggers the ENC blockade when ENC port or cable failure comes up and the ENC firmware download retry logic is executed. <Countermeasure> Modifying the ENC firmware download retry logic to work the dowload retry properly and to prevent ENC blockade for the ENC port or cable failure. <Action in the case of the failure> Exchange the ENC and ENC cable.	
	21	C	B	-	V93-S016	Countermeasure to controller failure during SnapShot(SS) restore	[Phenomena] There are cases where a controller fails with the message below when multiple drives having a SS pool fail during SS restore HJ1651 Microprogram error[RCF] <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) SS is enabled (2) SS restore is running (3) SS pair status transition to PSUE due to multiple drive failures [Cause] Firmware bug. A controller failure occurs because there is a problem with the process of changing information for differential data when the SS pair status transitions to PSUE due to multiple drive failures. <Countermeasure> The process of changing information for differential data is modified so that a controller failure does not occur. <Action in the case of the failure> (1) Perform dummy replacement of the controller to recover the controller. (2) Delete the SS pair whose status is PSUE and then create the SS pair again.	
	22	C	B	-	V93-0030	Dynamic Provisioning Illegal notification by E-mail alert and SNMP when "the current value exceeds threshold" occurred.	[Phenomena] "Send notification by E-mail alert and SNMP if the current value exceeds threshold" is disable,but Send notification by E-mail alert and SNMP. <Equipment model / Firmware version> DF800S/M/H, V7.0/A(0870/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)DF800EH/EM/ES/H/M/S (2)Dynamic Provisioning is used (3)SNMP Agent Support Function is used (4) E-mail alert is used (5)"Send notification by E-mail alert and SNMP if the current value exceeds threshold" is disable [Cause] Firmware bug. When function of Alert Threshold of the DP Pool Usage Capacity is disable, the firmware notified E-Mail/SNMP incorrectly. <Countermeasure> The firmware refer to the management table,when Send notification by E-mail alert and SNMP. <Action in the case of the failure> Ignore a notification by E-mail alert and SNMP.	

	23	C	B	-	V93-B024	Illegeal drive failure occurs in Dynamic Provisioning Pool Volume after drive recovery completion	[Phenomena]
							Drive failure for LA error occurs in HDP pool after drive recovery completed.
							
							<Equipment model / Firmware version>
							DF800S/M/H, V7.0/A(0870/A) or later
							DF800ES/EM/EH, V9.0/A(0890/A) or later
							
							[Conditions of Occurrence]
							The problem may occur when all following conditions are met.
							(1)Using Hitachi Dynamic Provisioning
							(2)The drive which is configured by DPRG is under recovery.
							(3)Any condition shown below.
							  1)Shadow Image or Modular Volume Migration on Hitachi Dynamic Provisioning
							  2)Data reclaim on configuration of Symantec (Issue the Write Same command) with Hitachi Dynamic Provisioning
							(4)Host I/O on the Hitachi Dynamic Provisioning volume	

							[Cause] Firmware bug. There may be the case that recovery unfinished areas in Hitachi Dynamic Provisioning pool are left after drive recoverey completed. And when the data is read for Host access, drive failure for LA error occurs. <Countermeasure> Modifying the logic in drive recovery not to skip the recovery in all area in Hitachi Dynamic Provisioning pool. <Action in the case of the failure>	
	24	C	C	-	V93-B006	Countermeasure to the problem of being unable to set the attribute which prohibits write operation to the ShadowImage(SI) P-VOL in PSUS(SP) status.	[Phenomena] Using Data Retention Utility(DRU), the attribute which prohibits write operation can not be set to the SI P-VOL in PSUS(SP) status. <Equipment model / Firmware version> DF800S/M/H, V6.2/A(0862/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Both SI and DRU are enabled (2) The SI pair status is PSUS(SP) [Cause] Firmware bug. Setting the write inhibit attribute to SI P-VOL in PSUS(SP) is prohibited like S-VOL in the same way for the S-VOL. <Countermeasure> The firmware is modified so that the write inhibit attribute can be set to SI P-VOL in PSUS(SP). <Action in the case of the failure> Wait until the pair status changes from PSUS(SP) to PSUS where the attribute can be set to the P-VOL.	
	25	C	C	-	V93-B006	Countermeasure to the problem that command devices can not be set up on multiple Hitachi Storage Navigator Modular 2(HSNM2) PCs.	[Phenomena] There are cases where when trying to set up command devices on multiple HSNM2 PCs almost at the same time, only the last command device can be set up while the other command devices are not set up. <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Multiple HSNM2 PCs is executed (2) Command device numbers are registered on multiple HSNM2 [Cause] Firmware bug. Because there is a problem with the process of registering command device numbers exclusively when those numbers are being registered almost at the same time on multiple HSNM2, the information of command devices which have already set up is overwritten improperly. <Countermeasure> The firmware is modified so that the information of command devices which has already set up can not be overwritten unless those command devices have been deleted. <Action in the case of the failure> Confirm the command devices on the subsystem. If command devices you need eventually have not been set up, release	
	26	C	C	-	V93-S009	Countermeasure to the problem that synchronization rate is incorrectly displayed during TrueCopy(TC) re-synchronization	[Phenomena] There are cases where 0% is displayed even while copy is progressing during re-synchronization. <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) TC is enabled (2) The size of the LU is not multiples of 32GB (3) Resync operation is performed after the pair status becomes PSUE due to PS OFF with cache volatilization on the remote array, Or swap operation is performed after the pair status becoomes PSUE due to PS OFF with cache volitilization on the local array. (4) Pair status is referred on Hitachi Storage Navigator Modular2	

							[Cause] Firmware bug. In the process of merging differential information on the local and remote arrays to calculate synchronization rate for TC, there is a problem with the completion process of progress of the final block and there are cases where calculated results of synchronization rate exceed 100%. (0% is displayed for synchronization rate) <Countermeasure> Correct the completion process for progress of the final block not to count the synchronization rate incorrectly. <Action in the case of the failure> Reference pair status again.
	27	C	C	-	V93QA005	Countermeasure to the problem that synchronization rate is incorrectly displayed when referencing pair status of TrueCopy(TC), ShadowImage(SI) or Modular Volume Migration(MVM)	[Phenomena] There are cases where synchronization rate is incorrectly displayed when referencing pair status on Hitachi Storage Navigator Modular2(HSNM2) or RAID Manger(RM). <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) TC, SI or MVM are enabled. (2) An LU of 41TB or more is part of a TC, SI or MVM pair. [Cause] Firmware bug. Overflow occurs during culculation because there is a problem in calculating synchronization rate. <Countermeasure> The process of calculating synchronization rate is corrected. <Action in the case of the failure> Ignore the display of uncorrect synchronization rate because this is a display problem.
	28	C	C	EUC1196375	V93-S001	Countermeasure for illegal message when executing the LU expanding after shrinking the same LU.	[Phenomena] The following message may be reported inappropriately at the timing of Array reboot after expanding the LU which has been once shrunk. Unformatted area remains in the LU(LU-XXXX). Please contact support for assistance <Equipment model / Firmware version> DF800S/M/H, V8.5/F(0885/F) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Executing the LU shrinking (2) Expanding the LU which has been once shrunk. (3) Referring the LU status by HSNM2 during the Quick formatting of expanded LU area. (4) After completing above Quick Format, executing one of [Cause] Firmware bug. Although both of "Quick Format progress status" and "LU capacity information" must be updated simultaneously, there is a case that the only the "LU capacity information" is updated. This causes the status inconsistency, then reports above message inappropriately. <Countermeasure> Modifying the logic to update both information simultaneously every time. <Action in the case of the failure> Backup the LU data to somewhere and execute the LU format
	29	C	B	-	V93QA039	Controller blockade when receives ATS command in VMware configuration	[Phenomena] When VMware server issues Write Command just after the ATS command, the controller blockade may occurs with the web following message. W1K001 Data transfer checkerror[SEGPOSERR] <Equipment model / Firmware version> DF800S/M/H, V9.0/A(0890/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Using VMware configuration (2) Receiving Write command within 5 second just after ATS command receipt on the same address (3) Using in VMware vSphere 4.1 or later system

							[Cause] Firmware bug. When data for ATS command is written to cache memory, an invalid bit in reserved field of Data Check Code may be on. Controller blockade may occure due to checking the invalid bit when receiving Write command just after the ATS command receipt in the same address typically issued in VMware configuration. <Countermeasure> Firmware fix the bug with correcting of Data Check Code for ATS command data.			
	V9.3/B, 0893/B							7/21/2010	247	None
V9.3/B 0893/B Base System V9.3/A, 0893/A	1	C	A	SD3158976	V93-0176	When Data Transfer LSI failure occurred on a controller, an access lost may occur on another controller.	[Phenomena] When Data Transfer LSI failure occurred on a controller with the following web message, an access lost may occur on another controller. H06D0x [DCTL]The PCI root complex error wasdetected [E_IRQ6](CTL-x) <Equipment model / Firmware version> DF800/H, V3.2/A(0832/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. [Cause] Firmware bug. There is a problem in the process of exchanging information between controllers when Data Transfer LSI on a controller failed. <Countermeasure> The process of exchanging information between controllers is modified. <Action in the case of the failure> (1) Replace the blocked controller with Data Transfer LSI failure. (2) Perform a power cycle.			
	2	C	B	EUC1155694	V93-0156	An access lost may occur when Dynamic Sparing process is running caused by many errors on an HDD.	[Phenomena] Dynamic Sparing process runs with the following web message (A) caused by many error on an HDD. Then, host detects many command time-outs at the LUs including the failed HDD, and finally an access lost occurs. After that, the HDD blockade occurs with the following web message (B) caused by too many errors on the failed HDD and Correction Copy process runs with the following web message (C). So host access recovers. WEB message (A): "I15Axy Dynamic sparing start", "I150xy Data recovery started" (B): "HDU alarm", "I152xy Data recovery failed" (C): "I150xy Data recovery started" <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Dynamic Sparing process runs caused by many errors on an HDD. [Cause] Firmware bug. When many errors are detected on a failed HDD during Dynamic Sparing process, Dynamic Sparing process is continued to run wrongly. Therefore many command retry processes run and I/O processes slow down. <Countermeasure> Correction Copy process is run instead of Dynamic Sparing process for data recovery, when more errors are detected on a failed HDD during Dynamic Sparing process. <Action in the case of the failure> Please replace a failed HDD during Dynamic Sparing.			
	3	C	B	SD3208905	V93-0179	Controller blockade may occur during array unit booting.	[Phenomena] When a power cycle is performed, a controller blockade may occur with the following web message. H90320 Watch-dog time-out <Equipment model / Firmware version> DF800S/M/H, V7.0/A(0870/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Hitachi Dynamic Provisioning function is used. (2) Any one of the following operation is executed. ・Power cycle.			

							[Cause] Firmware bug. When HDP is used, a cache access is slow wrongly during power up process, so a controller blockade may occur caused by watch-dog time-out. <Countermeasure> This problem was modified that the access mode of the cache memory operated correctly when HDP is used. <Action in the case of the failure> Please perform a dummy-replacement of the blocked controller.	
	4	C	B	SD3200692	V93-0178	Read/Write performance may be degraded because of SyncCache commands	[Phenomena] When subsystem received a lot of SyncCache commands and Read/Write commands in short period, it is possible that CPU utilization increase and host I/O performamce may be degraded, even if Synchronize Cache Execution Mode is disable. <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)System parameter, Synchronize Cache Execution Mode, is disable. (2)A lot of SyncCache commands are received [Cause] Firmware bug. When Syncronize Cache Execution Mode is disable, SyncCache command should be no operation. However Read/Write commands are wrongly excluded and watied by SyncCache command. <Countermeasure> When subsystem receives a SyncCache command in the case of Syncronize Cache Execution Mode is disable, subsystem deal SyncCache command as NOP. <Action in the case of the failure>	
	5	C	B	SD3166844	V93-0174	A linkup failure may occur after non-disruptive firmware update.	[Phenomena] A linkup failure may occurs after non-disruptive firmware update under a link down and Fibre Channel signal receipt state <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)Fibre Channel I/F deployment Port (2)The state is Link Down even though a Fibre Channel signal is received (3)Non-disruptive FW update is performed under condition (1) and (2). [Cause] Firmware bug. Non-disruptive firmware update included the malfunction that cable connection search processing did not work for a port which the state is Link Down even though Fibre Channel signal is received. Therefore Link Up state cannot be detected by cable connection after Non-disruptive firmware update. <Countermeasure> A cable connection search is performed without relation in the receipt of a signal. <Action in the case of the failure> Please excute any one of the following operation. (1)By a setting the Fibre Channel Information change transfer speed. ・case of "Auto"　: Change it in "fixation" once and return it to "Auto". ・case of "fixation"　: Change it in "Auto" once and return it	
	6	C	B	-	V93-0177	ENC may be blocked wrongly when a hardware error of SAS controller occurs.	[Phenomena] ENC in RKA failure occur wrongly when the route diagnosis on backend is running. <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)There are SAS HDUs in RKA. (2)Hardware error in SAS controller occur.	

							[Cause] Bug of SAS Controller Firmware SAS controller wrongly detects an internal hardware error of ENC while accessing SAS HDU. So, ENC error count is over the threshold, then the ECN is blockaded. <Countermeasure> SAS controller firmware is corrected. <Action in the case of the failure> Please perform a dummy-replacement of the blockaded ENC. Please exchange controllers connected with ENC when failure occurs again.
	7	C	B	-	V93-0168	The controller blockade may occur when a host command is received without a login process.	[Phenomena] The controller blockade may occur with the following web message when a host command is received without a login process. HOZONOx Kernel processing error (CTL-x) <Equipment model / Firmware version> DF800S/M/H, V4.0/A(0840/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Fibre Channel I/F (2) Installing LUN Manager function and available (3) The target Host's WWN is not registered in Host Group. (4) A target host is never connected. [Cause] Firmware bug. There was a problem in the reference to the table, when the PDISC command was accepted. Because the processing of the memory access at infinity had been executed, the controller blockade was occurred. <Countermeasure> When the PDISC command was received, the firmware bug was corrected that the table reference was correctly acquired. <Action in the case of the failure> Please perform a dummy repalcement of the blocked controller.
	8	C	B	-	V93-B026	Controller and SAS HDU are blockaded wrongly when SATA HDU is removed and then SAS HDU is inserted to the same slot.	[Phenomena] When SATA HDU is removed and then SAS HDU is inserted to the same slot, controller failure and inserted SAS HDU failure may occur with the following web message. <Information Message> W093ZZ HDU alarm(Unit-Y,HDU-Z,Type-Unknown):HDU I30400 HDU spin up failed(Unit-Y,HDU-Z) W0130X CTL alarm(CTL-X) :CTL H30K00 Backend error count of the CTL was over the threshold[CODE-2E](CTL-X) :CTL X: Number of Controller Y: Number of Unit Z: Number of HDU <Equipment model / Firmware version> DF800S/M/H, V7.2/A(0872/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when SAS HDU is replaced. [Cause] Firmware bug. Intermittent hardware errors occur when SATA HDU is removed. After that, when SAS HDU inserted to the same slot, firmware handles the inserted SAS HDU as SATA HDU wrongly. HDU spin up processing only for SATA drive is executed. The response from SAS drive was judged to be an abnormal response of SAS controller. So, Controller failure occurs. Also, SAS HDU failure occurs because it fails spin up processing. <Countermeasure> Judgment logic of HDU type when the HDU is inserted is corrected. <Action in the case of the failure> Please perform a dummy replacement of the blocked controller. Please perform a dummy replacemet of the blocked SAS HDU.
	9	C	B	-	V93-S038	WEB cannot be connected by controller blockade when PS/ON is executed.	[Phenomena] WEB cannot be connected by controller blockade when PS/ON is executed at iSCSI mounting array. <Equipment model / Firmware version> DF800H/ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)DF800H/ES/EM/EH (2)The iSCSI I/F board is installed in I/F slot#1. (3)The controller blockade is occurred while the array is booted.

							[Cause] Firmware bug. When the controller blockade was occurred during the array was booted, and before the array initializes the iSCSI chip, a hard reset was performed to an unexiting port based on an uncertainly port information. As a result, the controller hangs up, and the WEB connection could not be connected. <Countermeasure> The hard reset is executed at iSCSI chip, when the port information had been correctly set.	
	10	C	B	-	HDS-0105	A remote path can not recover automatically.	[Phenomena] When arrays are connected through Fibre Channel Switchs (FC-SW) for remote replication, pulling out a FC cable from the remote array causes a remote path failure with the following message. Subsequently when the FC cable is connected to the array again, the remote path on the side of the remote array automatically recover but the remote path on the side of the local array does not automatically recover. Only the remote path on the controller 1 does not recover. <Equipment model / Firmware version> DF800S/M/H, V9.0/A(0890/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] When all of (1)-(3) conditions are met and the following (4) or (5) is met, the problem occurs. [Cause] Firmware bug. There is a problem with the remote path recovery process. In the process to wait 15 seconds after a link failure in order to avoide a remote path failure due to a temporary link failure, the path recovery process is not properly performed, so the remote path does not automatically recover <Countermeasure> The firmware is modified so that a failed remote path can recover properly when the remote path recovery process is working. <Action in the case of the failure> Recover the remote path manually via SNM2 or web tool.	
	11	C	C	-	V93-0160	The counter of Phy Error Log is traced wrongly in simple trace or full dump. Phy Error Log counter: Counter of hardware error of SAS devices.	[Phenomena] The counter of Phy Error Log of follow devices is traced wrongly in simple trace or full dump. ・Expander0 in Controller 0 ・Expander1 in Controller 1 ・SAS controller counter of Path 0 in Controller 0 ・SAS controller counter of Path 1 in Controller 0 ・SAS controller counter of Path 2 in Controller 0 <Equipment model / Firmware version> DF800H, V5.0/A(0850/A) or later DF800EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)DF800H/EH (2)Hardware error on backend route occurs at the follow timing. ・Search for the backend route error is run on other path ・Firmware exchange ・Controller insert [Cause] Firmware bug. The hardware error counter initialization processing is wrong. A clear range is specified by mistake, and the following counter values become wrong. ・Expander0 in Controller 0 ・Expander1 in Controller 1 ・SAS controller counter of Path 0 in Controller 0 ・SAS controller counter of Path 1 in Controller 0 ・SAS controller counter of Path 2 in Controller 0 <Countermeasure> A clear range of the counter is correctly set. <Action in the case of the failure> No influence in the operation of the array. (Trace information only)	
	12	C	C	-	V93-0175	CPU Load Reduction for Cross-CTL I/O Mode guard for DF800EH	[Phenomena] Performance down may occur (around 10%) when "CPU Load Reduction for Cross-CTL I/O Mode" is set to enable wrongly in DF800EH. Also, the option menu is displayed on othet than DF800H. <Equipment model / Firmware version> DF800EH, V9.0/B(0890/B) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)DF800EH (2)CPU Load Reduction for Cross-CTL I/O Mode is effective	

							[Cause] Firmware bug. There was not the guard that did not work in DF800EH with CPU Load Reduction for Cross-CTL I/O Mode.In addition, and the option menu was displayed on other than DF800H. <Countermeasure> CPU Load Reduction for Cross-CTL I/O Mode is detered in DF800EH. The option menu is not displayed on other than DF800H. <Action in the case of the failure> When use DF800EH, don't use CPU Load Reduction for Cross-CTL I/O Mode.			
	V9.3/D, 0893/D							8/16/2010	256	None
V9.3/D 0893/D Base System V9.3/B, 0893/B	1	C	A	EUC1226911	V93-0194	Data inconsistency of HDP volume may occur after DP Optimization.	[Phenomena] The customer uses LVM(logical volume manager) mirroring on AIX for Oracle DB by using 2 DF800. When a consistency check was performed, data inconsistency (*1) of HDP volume was detected. *1: Around 2,000 blocks (4Kbyte per block) are all "00". <Equipment model / Firmware version> DF800S/M/H, V8.0/A(0880/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)Hitachi Dynamic Provisioning function is used. (2)DP Optimization was performed (Example adding a DP pool capacity, LU shrink, DP Optimization by manual.) (3)DP Optimization was canceled via SNM2, or skipped due to migration timeout cause by a heavy write load from a host. The problem may occur when all of the above conditions are met and any of the following condition is met. <V8.x is installed.> (4)Shutdown (5)Firmware update to V9.x <V9.x is installed.> (4)Shutdown (5)Firmware Exchange [Cause] Firmware bug. The firmware bug of DP optimization A migration running status flag for Page Address (*2) may be not cleared wrongly when DP optimization is canceled via SNM2 or skipped due to a migration timeout caused by a heavy write load from a host. Then the Page Address, which migration running status flag is still set wrongly, is linked to the other LU or the other address. After that, when a firmware exchange or a shutdown and so is performed, the Page Address is deleted wrongly. In the result, when user data related with the Page Address is read, all "00" data is transferred because a firmware judges wrongly that a target data is unused (no data). *2: Real user data address is linked by Page Address information for a DP Pool. <Countermeasure> When the migration running state flag in the state in the state of being set wrongly is cleared while a firmware exchange, and the DP optimization function is interrupted, the flag is not left wrongly.			
	V8.5/H, 0885/H							8/27/2010	264	None
V8.5/H 0885/H Base System V8.5/F, 0885/F	1	C	-	EUC1226911	V85-0101	Data inconsistency of HDP volume may occur after DP Optimization.	[Phenomena] The customer uses LVM(logical volume manager) mirroring on AIX for Oracle DB by using 2 DF800. When a consistency check was performed, data inconsistency (*1) of HDP volume was detected. *1: Around 2,000 blocks (4Kbyte per block) are all "00". <Equipment model> DF800H/M/S <Firmware version> V8.0/A(0880/A) or later [Conditions of Occurrence] The problem may occur when following conditions are met. (1) Dynamic Provisioning function is used. (2) DP Optimization was performed (Example adding a DP pool capacity, LU shrink, DP Optimization by manual.) (3) DP Optimization was canceled via SNM2, or skipped due to migration timeout cause by a heavy write load from a host. The problem may occur when all of the above conditions are met and any of the following condition is met. <V8.x is installed.> (4) Shutdown			

							[Cause] Firmware bug. The firmware bug of DP optimization A migration running status flag for Page Address (*2) may be not cleared wrongly when DP optimization is canceled via SNM2 or skipped due to a migration timeout caused by a heavy write load from a host. Then the Page Address, which migration running status flag is still set wrongly, is linked to the other LU or the other address. After that, when a firmware exchange or a shutdown and so is performed, the Page Address is deleted wrongly. In the result, when user data related with the Page Address is read, all "00" data is transferred because a firmware judges wrongly that a target data is unused (no data). *2: Real user data address is linked by Page Address information for a DP Pool. [Countermeasure] If DP optimization canceled or skipped, the migration running status flag is cleared. After firmware exchange, checks and clears the invalid flag.When the check operation is started, the following web message is shown. "Start to check DP management information." - When the invalid flag is cleared, the following web message is shown. "The DP invalid flag was cleared. Please contact support for assistance."			
	V9.3/E, 0893/E							8/31/2010	258	022
V9.3/E 0893/E	1	N	-		V93-0190	System tuning parameter is added.	Dirty data flush number limit is supported.			
	2	C	A	EUC1226911	V93-0194	Data inconsistency of HDP volume may occur after DP Optimization.	[Phenomena] The customer uses LVM(logical volume manager) mirroring on AIX for Oracle DB by using 2 DF800. When a consistency check was performed, data inconsistency (*1) of HDP volume was detected. *1: Around 2,000 blocks (4Kbyte per block) are all "00". <Equipment model / Firmware version> DF800S/M/H, V8.0/A(0880/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Hitachi Dynamic Provisioning function is used. (2) DP Optimization was performed (Example adding a DP pool capacity, LU shrink, DP Optimization by manual.) (3) DP Optimization was canceled via Hitachi Storage Navigator Modular 2(HSNM2), or skipped due to migration timeout cause by a heavy write load from a host. The problem may occur when all of the above conditions are met and any of the following condition is met. <V8.x is installed.> (4) Shutdown array (5) Update firmware to V9.x [Cause] The firmware bug of DP optimization A migration running status flag for Page Address (*2) may not be cleared wrongly when DP optimization is canceled via HSNM2 or skipped due to migration timeout caused by heavy write load from hosts. Then the Page Address, which migration running status flag is still set wrongly, is linked to the other LU or the other address. After that, when firmware update, shutdown, and so is performed, the Page Address is deleted wrongly. In the result, when user data related with the Page Address is read, all "00" data is transferred because the array judges wrongly that target data is unused (no data). *2: Real user data address is linked by Page Address information for a DP Pool. <Countermeasure> If DP optimization canceled or skipped, the migration running status flag is cleared. After firmware exchange, checks and clears the invalid flag. When the check operation is started, the following web message is shown. "Start to check DP management information." - When the invalid flag is cleared, the following web message is shown. "The DP invalid flag was cleared. Please contact support for assistance." - When the check operation completes, the following web message			

	3	C	A		V93-0196	Host access lost by ATS command from VMware improperly keeping memory area	[Phenomena] ATS command improperly keeps memory area when it is executed. Host access lost or drive recovery stopped occurs because depleted memory makes it impossible for operations to work that use the memory like host I/O and drive recovery. <Equipment model / Firmware version> DF800S/M/H, V9.0/H(0890/H) or later DF800ES/EM/EH, V9.0/H(0890/H) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) ATS commands are issued. [Cause] Firmware bug. When ATS command reads data from drives, it tries to re-obtain already saved memory area. However ATS command improperly re-obtains memory area without releasing the saved memory area. This results in unreleased memory area. <Countermeasure> ATS command releases all of the saved memory area when trying to re-obtain memory area. <Action in the case of the failure> Perform either (1) or (2). (1) Change the ownership of LU from Hitachi Storage Navigator Modular 2. (any LU is OK) (2) Shutdown and reboot the array.
	4	C	A	EUC1231703	V93-0199	LA Error may occur when RAID Group Expansion is executed.	[Phenomena] LA error may occur when RAID Group Expansion is executed. <Equipment model / Firmware version> DF800S/M/H/, V9.0/A (0890/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when the following condition is met. (1) RAID Group Expansion is executed. [Cause] Firmware bug. When LU owner change occurs at a LU, which is running RAID Group Expansion process, RAID Group Expansion process for the LU is wrongly finished. In the result, LA error occurs when a host accesses to blocks which have not been expanded. <Countermeasure> RAID Group Expansion is not canceled but stopped when LU owner change occurs during RAID Group Expansion process. <Action in the case of the failure> Please execute a forcible cancel of RAID Group Expansion via SNM2. The LU which has been running RAID Group Expansion process becomes un-format status.
	5	C	A		V93-0197	Subsystem down during booting of array in a single controller configuration	[Phenomena] Subsystem down may occur during booting of array in a single controller configuration with the following message. R2390x : [DCTL]The bridge error was detected[external access](CTL-#) <Equipment model / Firmware version> DF800S/M/H/, V9.3/B (0893/B) or later DF800ES/EM/EH, V9.3/B(0893/B) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Single controller configuration (2) Cache volatilization occurs by any of the following operations. (a) Remove controller while power is off . (b) Power on array while power is off. [Cause] Firmware bug. When power on the array while cache memory is volatilized, cache memory volatilization is recognized as hardware error when checking the status of cache memory. Even if it is single controller configuration, the DUAL-PCI register which is required for dual controller configuration is incorrectly accessed. The controller is blockaded by the access failure to the DUAL-PCI register and then the subsystem goes down. <Countermeasure> Unnecessary register access is not excuted when single controller configuration. <Action in the case of the failure> (1) Add another controller and boot the array while the mode is single mode. (2) Although the added controller is blockaded, the system becomes ready since it is in single mode. Message : RA6000 CTL

	6	C	A		V93-0200	Controller blockade during booting of array after power down while there are host I/Os to the LU which has RAID1 or RAID1+0 configuration.	[Phenomena] Controller may be blockaded with the following message during booting of array after power down while there are host I/Os to the LU which has RAID1 or RAID1+0 configuration. H90320 Watch-dog time-out W0R000 User data lost(LU-xxxxx) <Equipment model / Firmware version> DF800S/M/H/, V9.3/B (0893/B) or later DF800ES/EM/EH, V9.3/B(0893/B) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) LU meets all of the following conditions. (a) It has RAID1 or RAID1+0 configuration. (b) It belongs to the RAID Group which consists of SAS HDD or SSD (c) It is not a cache resident LU (d) It is not an S-VOL of ShadowImage pair whose status is Paired or Synchronizing (e) It is not a P-VOL or S-VOL of SnapShot pair whose status is Split or Reverse Synchronizing (f) Drive recovery is not in progress (2) Write commands are issued from hosts to the above LU [Cause] Firmware bug. If the array is powered down while write commands are issued to the LU which has RAID1 or RAID1+0 configuration and then booted, data on the cache are checked in recovery process. If the information prior to power down is used to determine cache hit or miss , an exception occurs and controller is blockaded. Also write data in the cache memory is lost. <Countermeasure> In the recovery process of the reboot sequence after power down, use recovered information to check cache memory. <Action in the case of the failure> Perform the following (1) and (2) (1) Dummy replacement of the blockaded controller (2) Power-off/on the array to recover the LU whose cache
	7	C	A		V93-0202	A controller blockade or timeout occurs when XCOPY command is issued.	[Phenomena] When XCOPY command is issued on a HDP 32MB page across two RAID groups, XCOPY command is incorrectly handled as samel RAID group. If the HDP page across two RAID groups is unallocated, a controller blockade or subsystem goes down occurs due to an excepution handling , or no response to host occurs due to deadlock in XCOPY command. <Equipment model / Firmware version> DF800S/M/H, V9.3/A(0893/A) or later DF800ES/EM/EH, V9.3/A(0893/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) The source LU and target LU for XCOPY are same and they are DP-VOL. (2) The DP Pool consists of multiple RAID groups. [Cause] Firmware bug. When XCOPY command is issued on a HDP 32MB page across two RAID groups, there is a firmware bug in determining whether source and target of XCOPY overlap. If source and target of XCOPY command are in the same DP Pool but on the different RAID groups in the DP pool, they are wrongly handled as the same RAID group . So, an exception occurs by referring invalid information about RAID group and the controller is blockaded. <Countermeasure> Countermeasure If source and target of XCOPY command are in the same DP Pool, the routine to check whether they are on the different RAID groups in the DP pool is added to the process to determine if the source and target for XCOPY command overlap. <Action in the case of the failure> At the time of controller failure: Dummy replacement of the blocked controller
	8	C	A	SD3274616	V93-0204	Subsystem down by Micro HDP during initial copy of TrueCopy	[Phenomena] Controller blockade by microprogram error[HDP] may occur during initial copy of TrueCopy pair using DP-VOL at the local array . If another controller takes over the process, the subsystem goes down by the same error. <Equipment model / Firmware version> DF800S/M/H, V8.0/A(0880/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] (1) Create, resynchrnoize, or swap of TrueCopy or TrueCopy Extended Distance pair. (2) Both P-VOL and S-VOL are DP-VOL (3) Copy pace is set to normal or fast. (4) The internal status includes one of the followings. (a) The pair data that is being transferred

							[Cause] Firmware bug. Controller is blockaded by detecting logical inconsistency because the array tries to use invalid address in seaching differential data when creating TrueCopy or TrueCopy Extended Distance pair using DP-VOL. If the other controller takes over the process and the same thing happens, the subsystem goes down. Also if network used for data transfer is unstable, because there is a similar problem that uses invalid address when data transfer needs retried, the controller is blockaded and the subsystem goes down. <Countermeasure> Correct value is set for address to seach differential data during initial copy or retry of data transfer.
	9	C	A		V93-0201	Subsystem down by executing parity recovery after array is power on with cache volatilized.	[Phenomena] Microprogram error is detected[HDP] occurs on both controllers, and subsystem goes down when executing parity recovery after the booting of array with cache being volatilized just after configuration is changed. Message: HJ4Axx Microprogram error was detected[HDP] <Equipment model / Firmware version> DF800S/M/H, V8.0/A(0880/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Hitachi Dynamic Provisioning function is used. (2)Delete DP-VOL with allocated pages, create a DP-VOL with the same LU number in another DP pool, and host I/O is issued to this LU. (3)Information is not completely evacuated to HDD which is triggered by configuration change from Hitachi Storage Navigator Modular 2 . [Cause] Firmware bug. Because power off with cache volatilized during transfer information evacuated by HDD, Page Address(*1)and transfer information disagree with it. And outbreak by having restored local memory in the cause by Page Address. (*1):Real user data address is linked by Page Address information for a DP Pool. <Countermeasure> When power on with cache volatilized and detected disagreement of Page Address and transfer information in advance, match it with transfer information and carry out contradiction recovery of Page Address. <Action in the case of the failure>
	10	C	A	SD3187840 SD3222647	V93-0195	Controller blockade or backend down caused by frequent LAN accesses with SSL(Secure Socket Layer)	[Phenomena] (1) or (2) occurs by SSL access during the security test to the LAN port of the array: (1) Controller blockade (Message: HZ0N00 Kernel processing error) (2) System goes down due to backend down(Message: HH8W00 Backend has been down[All the routes have been blockaded]) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when the following condition is met. LAN accesses with SSL to the array are done very frequently. (More than 80 accesses per second. Such a high rate may not [illegible] [Cause] Firmware bug. It is a bug due to the lack of the consideration for the verification on "Year 2010 Compliance with NIST Minimum Security Strength." On SSL communication, the enhancement of the encryption key length from 1024 bit to 2048 bit requires longer time to encrypt. If LAN accesses with SSL are done very frequently, Read/Write processes can not be executed and controller blockade or backend down may occur. <Countermeasure> When the CPU penetoration ratio for the main process (e.g. host I/O processing) is low, activities of SSL processing are restricted for a while. <Action in the case of the failure> If a security test (e.g.. port scan, security scanner test etc.) is running against the array, please stop the test. And then perform dummy replacement of the controller or

	11	C	B		V93-0189 V93-0203	After LinkDown at a FC port when a host reboots , LinkDown failure occurs at the other port on the interface board , and then LinkUp fails.	[Phenomena] In the configuration where multiple hosts connect to multiple ports on an I/F board, if LinkDown occurs on a port due to a event such as host reboot or disconnecting/connecting a cable, other ports on the same I/F board also go LinkDown and never become LinkUp. <Equipment model / Firmware version> DF800S/M/H, V8.0/A(0880/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] (1) Two or more hosts are connected on the same I/F board. (2) The channel speed setting of the FC port is "Auto". (3) Host reboot, PS OFF/ON, disconnect/connect a cable (This problem can occur on a 4Gbps/8Gbps FC I/F board) [Cause] Firmware bug. When a port goes LinkDown on a I/F board, Auto Negotiation process wrongly starts on other ports of the same I/F board which is a Link initialization process to manage the port speed of Fibre channel. As a result, the Link initialization does not complete and then the ports do not go LinkUp. <Countermeasure> The firmware is modified so that when a port goes LinkDown, the Auto Negotiation process does not start on the other ports. <Action in the case of the failure> Please change the transfer rate. (1) The setting is "Auto speed" : Please set to "Fixed channel speed" and then re-set to "Auto speed. (2) The setting is "Fixed speed" : Please set to "Auto speed and
	12	C	B		V93-0185	Access lost may occur in heavy load environment due to HDD failure which causes response delay.	[Phenomena] Access lost may occur in heavy load environment due to HDD failure which causes response delay. <Equipment model / Firmware version> DF800/S/M/H V3.2/A(0832/A) or later DF800/EH/EM/ES V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Failure occurs on HDD which results longer response time. (2) The load to the HDD is very high [Cause] Firmware bug. I/O becomes timeout due to delayed response by HDD and the array issues reset to the HDD. The commands issued at the same time are retried after the completion of reset but timeout occurs on another job and reset is issued again. This results in longer time to blockade HDD and then delayed response to the I/O issued to the LUs in the RAID group which contains the HDD. <Countermeasure> If the timeout occurs repeatedly on a certain HDD, the array blockades the HDD recognizing as a delayed response failure of HDD to prevent delayed response to the host I/O. <Action in the case of the failure> Replace the HDD with delayed response failure.
	13	C	B	SD3215292	V93-0184	Access lost occurs due to performance deterioration	[Phenomena] Access lost occurs due to performance deterioration <Equipment model / Firmware version> DF800S/M/H, V6.5/A(0865/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1)It takes more than 27 seconds to complete Read command. (2)Timeout / ABEND occurred during host data transfer. (3)The host issues reset command more than 27 seconds after [Cause] Firmware bug. If processing time of Read command exceeds 27 seconds, the array returns a check response as timeout. But a job gets terminated without sending the status response if timeout / ABEND occurs during host data transfer, and because the command stays in queue, the array becomes irresponsive. As a result, host access lost occurs. <Countermeasure> The array sends status response when timeout / ABEND occurred during host data transfer. <Action in the case of the failure> This problem may occur if response time per command is longer than 3 seconds but the commands are not shown in sink trace. Please recover by doing one of the followings. (1) Shut down and reboot the array. (2) Update firmware.

	14	C	B		V93-0182	HDD blockade status may be indicated wrongly by removing the HDD just after it is inserted.	[Phenomena] HDD is incorrectly indicated blockaded when the HDD is removed immediately after it is inserted and its LED is lit.The removed HDD is indicated blockaded on Hitachi Storage Navigator Modular 2 and indicated with alarm on web. <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) LU is not defined in the HDD [Cause] Firmware bug. The array incorrectly tries to access a HDD without checking whether it has been removed when the HDD is removed during the monitoring process after HDD insertion. <Countermeasure> Countermeasure The array checks whther HDD is inserted or removed or not before it actually access the HDD in the status monitoring process after HDD alarm LED is lit. <Action in the case of the failure> Perform one of the followings (1) Insert the HDD in a slot where it was removed from and remove it while avoiding the Condition of Occurrence (2).
	15	C	B		V93-0198	HDD blockade may occur due to incorrect threshold over by online verify.	[Phenomena] HDD blockade may occur due to incorrect threshold over by online verify. <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Skip online verify option is disabled (2) Errors are detected in multiple HDDs within an array by online [Cause] Firmware bug. Online verify checks error on all HDDs. If an error is detected, the error count is increased on the corresponding HDD. In the count up routine, the error count is increased for the HDD where the error is detected. However, in case that errors are detected in multiple HDDs at the same period of online verify, the error count up is wrong. <Countermeasure> The count up routine is corrected. <Action in the case of the failure>
	16	C	B		V93-0191	Fibre Channel port login(PLOGI) failure between an array and a host	[Phenomena] Host access lost may occur because PLOGI cannot complete when array and host are connected. <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Fibre Channel I/F (2) Loop topology is set on I/F port This phenomena has occurred on hosts of a certain type of a domestic vendor but never occurred on other general hosts (e.g. [Cause] Firmware bug. Host cannot access the array after PLOGI timeout because login process cannot continue when the fibre channel signal to control PLOGI may be depleted during the process of PLOGI form the host. <Countermeasure> Introduce a new port option named "PLOGI Timeout Prevention Mode": When the option is on, the time length of PLOGI process is monitored and the link is initialized if PLOGI cannot complete within one second. <Action in the case of the failure>

	17	C	C	EUC1196375	V93-0186	A web message "Unformatted area remains in the LU(LU-xxxx)" is shown falsely by firmware update after executing the LU shrink and expansion feature.	[Phenomena] A web message "Unformatted area remains in the LU(LU-xxxx)" is shown falsely by either of non-stop (online) firmware update, reboot of the array or online controller insertion after executing the LU shrink and expansion feature although LU format is completed and there is no problem in user data. <Equipment model / Firmware version> DF800S/M/H, V8.5/F(0885/F) DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) LU shrink is executed. (2) LU grow is specified to the LU that was shrunk. (3) LU status is referred using Hitachi Storage Navigator Modular 2 while the grown area of the LU is being formatted. (4) One of the following operations is done after the completion of the LU format. (a) Reboot the array(planned shutdown, power down with/without [Cause] Firmware bug. The bit count for format and the completed bit count of the quick format may differ even after quick format is complete. While this bug itself was fixed at V9.3/A (ECN DF800-239 Appendix-A #19), the inconsistency that had occurred in the array other than DF800H before V9.3/A was applied may display the message unnecessarily. <Countermeasure> Do the following (1) and (2) for DF800S/M and DF800ES/EM (1) Skip the check for the inconsistency of bit counters (2) TDCONV also skips the check. <Action in the case of the failure> For DF800S or DF800M, please apply the fixed firmware.			
	18	C	C	SD3235025	V93-0188	Reporting the full portal list of iSCSI Target that initiator can access it in the iSCSI discovery process.	[Phenomena] The AMS responses just for own port's IP address although the host(VMWARE ESX3.5) expects their full portal list of all the IP addresses on the port. <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1)iSCSI I/F (2)There is Target which registered iSCSI Name of initiator can [Cause] Firmware bug. Though all ports' information must be responded to the host in this single iSCSI discovery process, the AMS responses just for own port's information. <Countermeasure> Appending new target option(Report iSCSI Full Portal List Mode) . When this iSCSI target option is on , the all iSCSI Target information are reported to the host regardless of the port location where the discovery is received. <Action in the case of the failure> Set the iSCSI Target Name separately, and the IP address of all			
	V9.3/F, 0893/F							9/15/2010	267	None
V9.3/F 0893/F Base System V9.3/E, 0893/E	1	C	A		V93-0206	Controller failure or timeout may occur when XCOPY is issued to DP-Vol	[Phenomena] (a) A controller failure occurs with the following message. HJ4ABX Microprogram error was detected [HDP](CTL-X) System goes down when the failure occurs at both controllers. (b) A controller failure occurs without a factor message. Or, the following message is generated for the running controller if it tried to access the failed controller. HG0100 CTL communication send time-out System goes down when the failure occurs at both controllers. LAN access to the array is not possible. (c) Timeout error may be detected by a host. It may be recoverable by ABTS from the host. <Equipment model / Firmware version> DF800S/M/H, V9.3/A(0893/A) or later DF800ES/EM/EH, V9.3/A(0893/A) or later			

							[Conditions of Occurrence] Conditions of Occurrence 1 (Corresponding to Cause 1) The phenomenon (a) may occur if all of the conditions A to H are met. The phenomenon (c) may occur if all of the conditions A to G and I are met. A. The source and target of XCOPY command are a DP-VOL. B. The source and target of XCOPY command are in the same LU. C. The length of XCOPY command is less than 32MB D. The LU of the source and target of XCOPY command is a simplex volume. (The LU is not a part of replication PP pair.) E. The DP pool where the LU is made of multiple RG. F. RAID level of the DP pool is RAID5 or RAID6, and the number of data drives is other than 2D, 4D, 8D, or 16D G. The source of XCOPY command lies across two HDP pages and the tail of lock range overlaps with that for the target of XCOPY. Conditions of Occurrence 2 (Corresponding to Cause 2) The phenomenon (b) may occur if all of the conditions A to F are met. The phenomenon (c) may occur if all of the conditions A to E, G and H are met. A. The source and target of XCOPY command is a DP-VOL. B. The source and target of XCOPY command are in the same LU. C. The length of XCOPY command is less than 32MB. D. The LU of the source and target of XCOPY command is a simplex volume. (The LU is not a part of replication PP pair.) E. The LU is not LU0. F. LU0 is not in the array. G. LU0 is in the array. H. There are the job dealing with the case where source and target [Cause] Cause1 (Phenomenon (a) or (c) may occur): The problem is caused by the firmware bug related to XCOPY command which may be issued in ESX environment (VMware – vStorage). When a range of lock for source and target of XCOPY command is overlapped, they are adjusted due to avoiding of collision. In case that the LU is a DP-VOL, the virtual addresses of source and target need to be converted to actual allocation and then the ranges of lock are checked whether they overlap. When the LU is in a DP pool which is made of multiple RGs and the source of XCOPY command lies across two HDP pages, the array needs to check whether a tail of lock range for the source and lock rage for target overlap or not. However a head of lock range for source is wrongly used due to the firmware bug, and then an invalid area access or deadlock may occur. Cause2 (Phenomenon (b) or (c) may occur): The problem is caused by the firmware bug related to XCOPY command which may be issued in ESX environment (VMware – vStorage). When LU0 does not exist, and the source and target of XCOPY <Countermeasure1> The firmware is modified so that it is checked whether a tail of lock range for the source and lock range for target overlap or not. <Countermeasure2> The firmware is modified so that the appropriate DP-VOL information is set for a function when the source and target of XCOPY command lie across an HDP page boundary. <Action in the case of the failure> Phenomenon (a) or (b) Disable unique extended copy mode first and dummy replace the failed controller. In case of system down, perform a power cycle, and then disable unique extended copy mode. Phenomenon (c) If phenomenon (c) occurs repeatedly, perform a power cycle. (The commands stuck in the array due to deadlock are removed.) And then disable unique extended copy mode.	
	2	C	A		V93-0207	Controller failure may occur when online firmware update is executed.	[Phenomena] A controller failure occurs with the following message. HG0312 Resource release time-out <Equipment model / Firmware version> DF800S/M/H, V9.3/A(0893/A) or later DF800ES/EM/EH, V9.3/A(0893/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Online firmware update, firmware update with controller reboot, or controller insertion is executed.	

							[Cause] Firmware bug. A booting controller tries to obtain a chunk of 8MB cache memory area for initialization. When another contoller recieves SCSI commands other than Read/Write commands from the host, there is a possibility that 3 seconds timeout may occur on the controller when trying to obtain the shared resource. When it happened, the controller which failed to obtain the shared resource kills the booting controller. <Countermeasure> 8MB cache memory area is divided into eight 1MB blocks when allocated during controller initialization. The controller also waits for 1ms between successive 1MB allocation for making sure that the other controller can obtain the shared resource. <Action in the case of the failure> Dummy replace the failed controller.			
	V9.3/G 0893/G								9/28/2010	274	None
V9.3/G 0893/G Base System V9.3/F, 0893/F	1	C	B	SD3262240	V93-0208	Countermeasure for SATA HDD blockade, Enclosure failure, or Controller failure in mixed system of SATA HDDs and SAS HDDs	[Phenomena] SATA HDD, Enclosure in the additional unit, or Controller may blockade in mixed system of SATA HDDs and SAS HDDs. <Equipment model / Firmware version> DF800S/M, V3.2/C(0832/C) or later DF800H, V4.0/A(0840/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] When the following conditions occurred at the same time, this phenomena may be appeared. 1) SAS HDDs and SATA HDDs are mixed in the system 2) Heavy work load (especially Write IOs) on SAS HDDs 3) Write IO to SATA HDDs 4) Using HGST SAS HDDs in the system (*)Model Name(Mounted HDD) DF-F800-AKH146(HGST HUS153014VLS300 / HUS156030VLS600) DF-F800-AKH300(HGST HUS153030VLS300 / HUS144530VLS300 / HUS156030VLS600) DF-F800-AKH450(HGST HUS154545VLS300 / HUS156045VLS600) DF-F800-AKH600(HGST HUS156060VLS600) DF-F800-AKH450X(HGST HUS156045VLS600) DF-F800-AKH600X(HGST HUS156060VLS600) [Cause] SAS-Controller's Firmware bug. When many I/Os are issued to SAS HDDs and SATA HDDs, almost all Transmit Frame Buffers in SAS-Controller are in use by SAS HDDs access due to the firmware bug. SAS-Controller can't continue to send the upcoming data to SATA HDD(s) in this condition and SATA HDDs access timeouts may occur. The following failure may occur depend on the number of failed SATA HDDs or failed SATA HDDs position. - A SATA HDD blockade - Failure of Enclosure in the additional unit - Controller failure <Countermeasure> The fix of the SAS-Controller's Firmware. SAS-Controller will reserve a Transmit Frame Buffer to send upcoming SATA DATA not to occupy Transmit Frame Buffers for SATA HDD accesses. <Action in the case of the failure> If the replaced part is still blockaded, apply the fixed firmware.			
	V9.3/H 0893/H								10/14/2010	276	None
V9.3/H 0893/H Base System V9.3/G, 0893/G	1	C	A	SD3309672	V93-0209	Countermeasure of lost access to LUs due to SAS HDD failure	[Phenomena] Access loss may occur in heavy load environment due to HDD failure which causes HDD responses delay. <Equipment model / Firmware version> DF800S/M/H, V3.2/C(0832/C) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) SAS HDD (2) Medium Errors occur on HDD, and dynamic sparing starts. (3) Continued medium errors occur on write commands that have			

							[Cause] Firmware bug. When dynamic sparing starts, firmware stops to execute all host I/Os, and waits completion of all I/Os to HDDs.When continued Medium Errors occur on SAS HDD, these errors result longer response time for HDD I/O. There is a bug which allows Firmware wait for completion of all commands to the HDD with longer response time. The bug causes fail of dynamic sparing start and server access loss. <Countermeasure> Firmware is modified to stop the commands to the HDD as soon as Medium Error occurs on the HDD. <Action in the case of the failure> Please replace the HDD with delayed response failure.	
	2	C	A		V93-0210	Controller may be blockaded when execute DP optimization with Zero Page Reclaim.	[Phenomena] (1) Controller may be blockaded with the following message, when execute DP optimization with Zero Page Reclaim. W0U0xy DMA error (DMA-y) (2) Unused capacity may not increase, when execute DP optimization with Zero Page Reclaim. <Equipment model / Firmware version> DF800S/M/H, V8.0/A(0880/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The phenomenon (1) may occur if all of the conditions listed A to G are met. The phenomenon (2) may occur if all of the conditions listed A to E, H and I are met. A. Dynamic Provisioning function is used. B. Cache Partition Manager function is used. C. DP-Vol is assigned with a cache partition of segment size 8kB. D.DP-Vol was used. E. The DP Optimization with zero page reclaim option is executed. F. DF800S/M/H/EXS/ES/EM/EH. G. RAID5/RAID6 and the number of data disk more than 4 [Cause] Firmware bug. (1) The maximum of a comparing table list is exceeded in error. (2) The zero data pages are not released in error. Countermeasure (1)The maximum value of DRR List is modified. (2)The zero data pages are correctly checked. <Action in the case of the failure> Phenomenon (1) 1) DP optimization is finished Please Reboot the array or replace the failed controller at dummy. After the controller is recovered, the other controller must be performed a dummy replacement. Please do not execute DP optimization with Zero Page Reclaim until the fixed firmware is applied. 2) DP optimization is not finished Please cancel DP optimization and replace the blockaded controller at dummy. After reboot the array or the controller is recovered, the other controller must be performed a dummy replacement. And please do not execute DP optimization with Zero Page Reclaim until the fixed firmware is applied. Phenomenon (2) Please do not execute DP optimization with Zero Page Reclaim	
	V9.7/A, 0897/A							11/12/2010	268 None
V9.7/A 0897/A Base System V9.3/F, 0893/F	1	N	-	-	V97-0001	Restriction to reboot the Array when in installation and setting changes for Dynamic Provisioning, Copy on Write Snapshot and TrueCopy Extended Distance are removed.	Restriction to reboot the Array when in installation and setting changes for Dynamic Provisioning, Copy on Write Snapshot and TrueCopy Extended Distance are removed.		
	2	N	-	-	V97-0002, V97-0006	Enhancement of Dynamic Provisioning	-DP Capacity Mode is supported for RKS/RKM/RKH. -Accelerated Wide Striping Mode is supported. -DP Depletion Detail Reply Mode is supported.		
	3	N	-	-	V97-0003, V97-0082, V97-0249	SCSI specification with Dynamic Provisioning is updated.	SCSI specification with Dynamic Provisioning is updated.		
	4	I	-	-	V97-0008, V97-0048	Account Authentication improvement	This contains improvements, including the following: (a) Login IP address of each session that a user connects to the array is shown in the account list. (b) It is improved that a logged out user keeps available when a public account forcibly logs out the current user logged into the array.		
	5	I	-		V97-0132	Expanding the program stack area for firmware enhancement	Expanding the program stack area for firmware enhancement		
	6	I	-		V97-0113	Auto reboot function is improved so it will not work during online controller replacement.	Auto reboot function is improved so it will not work during online controller replacement.		
	7	I	-		V97-0012	Power Saving Integration (Flexible Host Check Cycle 0 - 720 min)	Power Saving Integration (Flexible Host Check Cycle 0 - 720 min)		
	8	I	-	EUC1166935	V97-0245	Improvement for the capturing trace data when Write command response time out (B/C006) occurs.	Improvement for the capturing trace data when Write command response time out (B/C006) occurs.		

	9	I	-	RASR0069	V97-0227, V97-0228	Improved backend diagnostic ability	Even if a failed part cannot be isolated, messages of candidate of a failed part can be displayed.
	10	C	A		V97-0257	ShadowImage(SI) pair can not be recovered after ShadowImage I/O Switching function activates	[Phenomena] A SI pair in Failure(S-VOL SwitchI) status can not be released. Also the pair can not be resynchronized and the pair can not be recovered. The following message appears when the S-VOL fails: W0Q000 LU alarm <Equipment model / Firmware version> DF800S/M/H, V1.0/A(0810A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) ShadowImage I/O Switching mode is enabled (2) SI P-VOL and S-VOL exist in different RAID groups. (3) S-VOL fails due to a double drive failure(triple drive failure for RAID6) to occur almost at the same time when pair creation/resync is specified, and then the S-VOL fails. (4) After (3), SI I/O Switching function activates when a double drive failure(triple drive failure for RAID6) occurs on the P-VOL [Cause] Firmware bug. Before pair status transitions to Synchronizing/Paired(pair creation/resync), the LU status is checked to make sure that pair creation/resync is executed only when the LU status is normal/regression. Because the preliminary LU status checking process and LU failure transition process do not make mutual exclusion, pair creation/resync can be inappropriately successful even in case a pair LU fails after the pair operation is specified. Subsequently if SI I/O Switching function activates due to a double drive failure(triple drive failure for RAID6) on the S-VOL, both the P-VOL and S-VOL become unformatted and then the pair can not be recovered. <Countermeasure> LU status is checked before the pair status transitions. And as a recovery procedure for the case that this problem has already occurred, when the pair status is Failure(S-VOL Switch) and the S-VOL is unformatted, the pair can transition to Failure so it can be released.
	11	C	A		V97-0257	Data inconsistency may occur between P-VOL and S-VOL when ShadowImage(SI) pairs in a Consistency Group(CTG) collectively transition to Split status	[Phenomena] When pair split is specified to a CTG including SI pairs whose status is Synchronizing/Paired Internally Synchronizing(Paired (IS)), if one of the following failures (*1) occurs on the P-VOL/S-VOL, the pair status incorrectly transitions to Split without completing the entire copy (*2). Although the identical rate of the pair can be displayed as 100% on Hitachi Storage Navigator Modular2(HSNM2), the data is actually not consistent between the P-VOL and the S-VOL. This problem does not occur when pair split is specified to a pair. <Equipment model / Firmware version> DF800S/M/H, V6.2/A(0862A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) SI is enabled (2) Pair status of the target pairs in a CTG is Synchronizing or Paired(IS) (3) Pair split is specified to the CTG (4) One of the following failures occur almost at the same time as the pair split (4)-1 PIN over occurs on the P-VOL or the S-VOL (4)-2 Drive Detach mode or ShadowImage I/O Switching mode is enabled Double drive failure(Triple drive failure for RAID6)occurs on the P-VOL. The problem does not occur due to S-VOL failure because [Cause] Firmware bug. The preliminary LU status checking process, and drive failure transition process or Failure transition process by PIN over do not make mutual exclusion. If drive failure or PIN over occurs after pair split is specified, the pair status should have transitioned to Failure but the pairs incorrectly transition to Split without completing the entire copy. <Countermeasure> It is confirmed that the pair status is not Failure before the pair transitions. If pairs in Failure status exist, the split operation is rejected

							<Action in the case of the failure> Please perform one of the procedures (1) to (3). (1) In case of PIN over (1)-1 Perform the recovery procedure for PIN over (1)-2 - When PIN over is resolved Resynchronize the pairs. - When PIN over is not resolved Release the pairs, format the LUs, and then restore backup data to the LU. (2) In case of double drive failure(triple drive failure for RAID6) (2)-1 Perform the recovery procedure for double drive failure(triple drive failure for RAID6) (2)-2 When PIN over is occurring, perform the recovery procedure for PIN over - When PIN over is resolved Resynchronize the pairs. - When PIN over is not resolved Release the pairs, format the LUs, and then restore backup data to the LU. (3) In case of LU failure	
	12	C	A		V97-0257	Host access lost occurs after completion of migration in Modular Volume Migration(MVM)	[Phenomena] Host access lost occurs after completion of migration in MVM. The following message appears when a reserved LU fails : "W0Q000 LU alarm" <Equipment model / Firmware version> DF800S/M/H, V1.0/A(0810A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) MVM is enabled (2) (a) or (b) is met (a) Drive Detach mode is enabled (b) ShadowImage I/O Switching mode is enabled and a SI pair exists in the same RAID group or DP pool as a reserved LU (3) A reserved LU fails due to a double drive failure(triple drive failure for RAID6) almost at the same time when migration starts [Cause] Firmware bug. Because the preliminary LU status checking process, and LU failure transition process do not make mutual exclusion, in case that a reserved LU fails after migration starts, the migration finishes with the migrated LU unformatted. At the time of completion of migration, I/O switches to the unformatted LU which results in host access lost. <Countermeasure> It is confirmed that a reserved LU does not fail when migration starts the actual copy. If the reserved LU fails at that time, the migration is forced to quit. <Action in the case of the failure> Please perform the procedures (1) to (6) when I/O is not available. (1) Release the MVM pair (2) Release the reserved LU (3) Replace the drives for the unformatted LU which is the former reserved LU. Format an LU and set it as a reserved LU (4) Execute migration (5) Release the MVM pair	
	13	C	A		V97-S028	Controller failure occurs when executing XCOPY command with a length of more than 16MB	[Phenomena] Controller failure occurs with the following message when executing XCOPY command with a length of more than 16MB. HJ11xx Microprogram error[RCH] When the host retries the same command, the same phenomenon occurs on the other controller and subsystem goes down. Or, performance degradation occurs if a portion of requested range of look-ahead read is not staged on the cache memory by reading a wrong data. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions 1-3 and either 4-1 or 4-2 are met. The phenomenon may differ depending on which of the conditions 4-1 or 4-2 is met. 1. the source of XCOPY command is DP-VOL 2. the length of XCOPY command is more than 16MB(the requested range of look ahead read is more than 32MB) 3. the requested range of look ahead read goes across 3 pages or more and the first and the last pages are allocated and pages in between are not. 4-1. The last page of a chunk is allocated to the page before an unallocated page in a DP-VOL. 4-2. A page other than the last page of a chunk is allocated to the page before an unallocated page in a DP-VOL.	

							[Cause] Firmware bug. The length of look ahead is set to be twice as long as the command length. Because the max length of look ahead is 32MB and the size of page is also 32MB, the number of pages that look ahead needs to read is considered to be 2. So, whether the page that needs to be read is already allocated or not is determined only on the first and the last page. However, when XCOPY command requests look ahead to read more than 32MB, the range of look ahead goes across 3 pages. When the allocation of the pages is allocated, unallocated, and allocated, the array will try to access an invalid area in the unallocated page and microprogram error[RCH] will occur. When the host retries the same command, the same phenomenon occurs on the other controller and the subsystem goes down. <Countermeasure> When the length of look ahead is calculated to be more than 32MB, the length is adjusted to 32MB. <Action in the case of the failure> Dummy replace the failed controller. Perform power cycle the array when subsystem occurred. None in case of performance degradation by reading data from
	14	C	A	SD3067226	V97-0234	When SAN boot is executed, the hung-up of OS is happened during disk scanning.	[Phenomena] When SAN boot is executed, the hung-up of OS is happened during disk scanning. <Equipment model / Firmware version> DF800S/M/H, V3.2/B(0832/B) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) AIX connection (2) LUN Manager function is used. (3) More than two hosts register to a host group. (4)One host responds and the check condition responds. (5)LOGO is done from another host. [Cause] Firmware bug. When the reset command is accepted, it is the microprogram bug that doesn't release the ACA. When reset is issued by the host which responds the check condition, the ACA is released. Therefore, even if the logout is accepted from another host, the state of ACA is not released. Originally, the range of the release of ACA is a unit of the host group. <Countermeasure> When logout is accepted, ACA to the host is cleared forcibly. <Action in the case of the failure>
	15	C	A		V97-B008	When a host read data in the state that DP Pool completely depleted, a host becomes Blue Screen Of Death.	[Phenomena] When data are written in a not yet allocate area in the state that a DP pool depleted The DP-VOL comes to do only a Check reply for a command from a host Therefore the host become Blue Screen of Death <Equipment model / Firmware version> DF800S/M/H, V8.0/A(0880/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) Dynamic Provisioning function is used. (2) DP Pool completely depleted (3)When data are written to a DP-VOL in a not yet allocate area in the state that a DP pool completely depleted. The problem may occur when all of the above conditions are met and any of the following condition is met. (4)Host read the data in the allocated area of the DP-VOL. [Cause] Firmware bug. When data are written in a not yet allocate area in the state that a DP pool depleted The DP-VOL comes to do only a Check reply for a command from a host <Countermeasure> If DP Depletion detail reply mode was ON, reply a Good Status for a lead command. <Action in the case of the failure>

	16	C	A		V97-0235	System copy is executed repeatedly and HDD isn't recovered when a HDD whose system area has media failure is inserted.	[Phenomena] "System copy start" and "System copy failure" are executed repeatedly and are not finished when a HDD whose system area has media failure is inserted. <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) System HDD is blockaded and the blockaded HDD is replaced to repair parts. System HDD = Any HDD from HDD(Unit#0,HDU#0) to HDD(Unit#0,HDU#4) (2) RG with HDD(1) has one or more LUs. (3) There is a media failure which will be occurred uncorrectable error response, if read, in system are on HDD(1). [Cause] Firmware bug. Firmware doesn't count up a threshold if firmware detected uncorrectable error when information is written in system area. If only the RG with System HDD has one or more LUs, "System copy start" and "System copy failure" are executed repeatedly. <Countermeasure> Firmware doesn't count up a threshold if firmware detected uncorrectable error when information is written in system area. If only the RG with System HDD has one or more LUs, "System copy start" and "System copy failure" are executed repeatedly. <Action in the case of the failure> Please replace the failure HDD which is executed system copy.	
	17	C	B		V95-0025	HDU failure occurs at the time of online firmware update for SAS drives	[Phenomena] SAS HDD failure in firmware updating during I/O. IZ0300 HDU update failed(Unit-XX,HDU-YY) W09zab HDU alarm(Unit-XX,HDU-YY,Type-c) <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Install SAS HDD(Viper-AP) firmware Ver.D06E or less. (2) Performing of online firmware update, firmware update with controller reboot, or online HDU firmware update. (3) I/O operations are being performed. [Cause] Firmware bug. When update the firmware of SAS HDU (Viper-AP), there is need to complete all I/O from both controllers on the target HDU. When only the controller issuing a HDU firmware update command ensures the completion of commands, the commands can remain uncompleted on the other controller. In that case, if the HDU firmware update command is handled before the uncompleted commands, drive failure may occur. <Countermeasure> Viper-AP firmware replacement is performed after both the controllers ensure the completion of I/O on themselves. <Action in the case of the failure> Web Message. HDU update failed(Unit-XX,HDU-YY) HDU alarm(Unit-XX,HDU-YY,Type-AKH146) (XX:Unit number,YY:HDU number) Please perform a dummy-replacement of the failed SAS HDU when the above message appears.	
	18	C	B		V97-B003	A host gets impossible to access the DP-VOL after virtual LU in DP Pool completely depleted was formatted.	[Phenomena] A host gets impossible to access the DP-VOL after virtual LU in DP Pool completely depleted was formatted. <Equipment model / Firmware version> DF800S/M/H, V8.0/A(0880/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)DP-VOL which received a command in the state that a DP pool completely depleted. (2)When carried out the following operation for the virtual LU, use rate of a DP pool has been more than 95% A. DP-VOL format B. Create DP-VOL of the same number after deleted DP-VOL	

							[Cause] Because 95% were less than it a capacity of use of a DP pool the opportunity that made an access restraint flag OFF <Countermeasure> When there was DP-VOL format or delete or creating, the access restraint flag is OFF. <Action in the case of the failure> Growing DP pool capacity,DP-VOL Delete or DP-VOL format,
	19	C	B		V97-0199	A controller is blockaded by a temporary controller obstacle in Program Product License Key operation	[Phenomena] A controller is blockaded by a temporary controller obstacle in Program Product License Key operation HJ1Fxx Microprogram error[PRO] <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)Dual Controller constitution (2)Program Product License Key Operation(Lock on/ Lock off/enable/disable) (3)Program Product License Key operation and a temporary controller obstacle coming at the same time. [Cause] In Program Product License Key operation, light processing works to flash memory of a controller of the other corollary with a controller of the operation execution side. When a temporary controller obstacle occurs at this time, a re-try works and publishes several communication processing. A re-try management table overflows at this time, and a controller is blockaded <Countermeasure> If other controller does not "Ready", Subsystem reply 5/2900. SNM Message: The specified function cannot be performed because the subsystem is in an incorrect status for execution. Please confirm there are no alarms/warnings in the subsystem, or the configuration is changed. <Action in the case of the failure> Dummy replace the failed controller and operate Program Product
	20	C	B		V97-0261	Controller failure occurs when iSCSI NOP-OUT commands received.	[Phenomena] Controller failure occurs when iSCSI NOP-OUT commands received frequently. HH7D58 Microprogram error[ISM] <Equipment model / Firmware version> DF800S/M/H, V1.0/C(0810/C) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions 1-2 are met. (1)iSCSI I/F (2)iSCSI NOP-OUT commands received frequently [Cause] Firmware bug. Receiving NOP-OUT commands frequently by external factor cause to run out of the resource for management information ,and microprogram error[ISM] will occur. <Countermeasure> <Action in the case of the failure> Dummy replace the failed controller.

	21	C	B		V97-0232	When the same IP address is set in the user management port and the default gateway by mistake, a controller failure occurs	[Phenomena] - Phenomenon which may occur at customer sites: Firmware version V8.0/A and later When the same IP address is set in the user management port and the default gateway by mistake, a controller failure occurs - Firmware version V6.0/A - V7.5/E When the same IP address is set in the user management port and the default gateway by mistake, network communication impossibility occurs. <Equipment model / Firmware version> DF800S/M/H, V6.0/A(0860/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. 1. Firmware version V6.0/A and later 2. The same IP address is set in the user management port and the default gateway. 3. SNMP function is enabling. 4. Trap reporting of SNMP. Trap reporting opportunity. - The Hardware failures occur. - disabled / enabled operation of SNMP from SNM2. - Config information re-setting of SNMP from SNM2. - Firmware exchange. - Restart the subsystem. [Cause] It is initialized an IP address of a default gateway in a network information table before published by Trap of SNMP, and is set it again. But when the same IP address value is set by a user management port and a default gateway, an IP address of a user management port is initialized, and controller blockade or network communication impossibility occurs. <Countermeasure> The logic to guard is added when the same IP address was going to be set by a user management port and a default gateway. <Action in the case of the failure> 1. Go to maintenance mode. 2. Change an IP address of a user management port or an IP address of a default gateway Web maintenance mode.	
	22	C	B		V97-0233	Controller blockade may occur without recovery process for SAS controller when SAS controller does not send any response.	[Phenomena] Controller blockade may occur without recovery process for SAS controller when SAS controller does not send any response. <Equipment model / Firmware version> DF800S/M/H, V6.5/A(0865/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) SAS controller becomes the fatal error state that SAS controller does not send any response. (2) Executing IO. [Cause] Firmware bug. When SAS controller does not send any response, firmware should reset SAS controller to recover it. But firmware does not reset SAS controller, so all IOs that send from the SAS controller become timeout. The count of IO timeout is over the threshold, and controller blockade occurs. <Countermeasure> When SAS controller does not send any response, firmware resets SAS controller to recover it. If SAS controller does not recover even if it was reset 3 times, firmware lets the controller blockade. <Action in the case of the failure>	
	23	C	B	SD3199496	V97-0091	In a configuration including Dense trays, when over maximum number of HDD slot (120 per path) may cause an incompletion of LU format.	[Phenomena] When over maximum number of HDD slot (120 per path), LU format does not complete with no error message in some configurations with Dense tray (i.e. RKAKX), although RAID Group can be created. <Equipment model / Firmware version> DF800S/M/H, V6.0/A(0860/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) DF800S/M/H/ES/EM/EH (2) The configuration with Dense tray (RKAKX). (3) The numbers of HDD slot are over 120 per path	

							[Cause] Firmware bug. The firmware has guard logic for maximum number of HDD slot as SAS chip specification (120 slot per path). However in case of some configurations with Dense trays, the guard logic cannot work. <Countermeasure> The guard logic for maximum number of HDD slot is modified correctly in case of some configurations with Dense trays. <Action in the case of the failure> (1) Please delete the LU whose format does not complete and the RAID Group which includes the LU. (The LU can be deleted though the format does not complete.)
	24	C	B		V97-0153	The disagreement between the capacity of the DP pool in HSNM2 and the DP pool capacity of Inquiry page E3h occurs.	[Phenomena] The disagreement between the capacity of the DP pool in HSNM2 and the DP pool capacity of Inquiry page E3h occurs. <Equipment model / Firmware version> DF800S/M/H, V7.0/A(0870/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1)Dynamic Provisioning function is used. (2)Creating a DP Pool. [Cause] The total pool capacity of Byte 34-41 and 42-49 of Inquiry Page E3h is wrong. <Countermeasure> To convert the dimension of capacity, 1024 is multiplied. <Action in the case of the failure>
	25	C	C		V97-0236	When Controller-1 blockade occurs, "controller-0" is displayed on Information Message that means cause of controller blockade.	[Phenomena] If PCI configuration process of SAS controller fails on controller-1, controller-1 blockade occurs. "HH7400 The backend PCI error count exceeded the threshold(CTL-0)" is displayed on Information Message. <Equipment model / Firmware version> DF800S/M, V3.2/C(0832/C) or later DF800H, V4.0/A(0840/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all following conditions are met. (1) PCI configuration process of SAS controller fails. (2) Even if firmware reset the SAS controller, PCI configuration process fail again. [Cause] Firmware bug. When controller blockade by hardware error in PCI configuration process of SAS controller occurs, firmware any time specifies "0" to controller number on Information Message. <Countermeasure> Firmware specifies a correct number of controller on Information Message. <Action in the case of the failure> The case, Information Messages of "HH7400 The backend PCI error count exceeded the threshold(CTL-0)" and "W01z01 CTL alarm(CTL-1)" are displayed at the same time, perform the
	26	C	C		V97-B012	Only one ShadowImage(SI) pair is splitted when splitting multiple SI pairs in the group using Consistency Group(CTG).	[Phenomena] When splitting the multiple SI Synchronizing pairs in the group using the CTG, only one Synchronizing pair is changed to Split after changed to Paired but the other pairs are not changed to Split. The pair which is changed to Split is different in the interface. ・When operated with Hitachi Storage Navigator Modular 2 (HSNM2) The pair has the smallest logical unit number in the SI pairs group used the CTG. ・When operated with RAID Manager The pair is written in the top of configuration definition file. <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) SI is enabled (2) Using the CTG when SI pairs are created. (3) SI pairs includes the pair whose status is Synchronizing. (4) Splitting the pairs in the group using the CTG with RAID Manager, or splitting the selected pairs with HSNM2

							[Cause] There is a firmware bug in the process after checking pair status in the group. If the pair status that is checked first is Paired when the splitting the SI pairs in the group using the CTG, the other pair status is checked. If all of the pair status in the group is Paired, the splitting using the CTG is performed. If the pair status checked first is Synchronizing when the splitting using the CTG, the other pair status is not checked and the only pair whose status is checked first is splited. <Countermeasure> The firmware is modified so that Check Response is received when an object of the splitting using the CTG is pair group which includes the pair whose status is Synchronizing, and the spiting using the CTG is performed only when an object is pair group which includes this pair whose status is Paired or Paired Internally Synchronizing. <Action in the case of the failure> (1) Resynchronize the pair whose status was changed to Split. (2) Split the pairs in the group using the CTG after all of their status in the group have been changed to Paired.			
	V9.7/B, 0897/B							11/12/2010	277	None
V9.7/B 0897/B Base System V9.7/A, 0897/A	1	I	-	-	V97-0265	Dynamic Provisioning Pool 64KB Stripe Size support	Dynamic Provisioning Pool 64KB Stripe Size support			
	2	I	-	-	E10-0437	Improvement for tracing ENC firmware log of ENC failure.	Improvement for tracing ENC firmware log of ENC failure.			
	3	C	A	SD3309672	V97-0268	Countermeasure of lost access to LUs due to SAS HDD failure	[Phenomena] Access loss may occur in heavy load environment due to HDD failure which causes HDD responses delay. <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) SAS HDD (2) Medium Errors occur on HDD, and dynamic sparing starts. (3) Continued medium errors occur on write commands that have not been executed when dynamic sparing starts. [Cause] When dynamic sparing starts, the firmware stops executing all host I/Os while waiting for completion of all I/Os to HDDs. When continued Medium Errors occur on SAS HDD, these errors result longer response time for HDD I/O. There is a bug which allows Firmware wait for completion of all commands to the HDD with longer response time. The bug causes fail of dynamic sparing start and server access loss. <Countermeasure> Firmware is modified to stop the commands to the HDD as soon as Medium Error occurs on the HDD when dynamic sparing starts. <Action in the case of the failure> Please replace the HDD with delayed response failure.			
	4	C	A		V97-0262	Controller failure occurs when DP-VOL is received reassigned command	[Phenomena] Controller failure occurs when DP-VOL is received reassigned command <Equipment model / Firmware version> DF800S/M/H, V7.0/A(0870/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. [Cause] Did not make processing NOP when DP-VOL is received reassigned command <Countermeasure> Make processing NOP when DP-VOL is received reassigned command <Action in the case of the failure> (1)controller failure occur Dummy replace the failed controller . (2)Subsystem is down			

	5	C	A		V97-0266	A controller blockade with Target abort INT status error in host I/O	[Phenomena] A controller blockade with Target abort INT status error in host I/O <Equipment model / Firmware version> DF800S/M/H, V5.2/A(0852/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1)SA800, DF800S/M/H,DF800EXS/ES/EM/EH (2) I/F is Fibre Channel [Cause] Set a reset flag by Host I/F Chip reset processing to execute in hard error(Target abort INT status error), but did not clear the flag with reset recovery processing. Countermeasure Clear the flag when reset processing was finished. <Action in the case of the failure> Dummy replace the failed controller . When load of host I/O is high, please lower load. Please carry out a review of a course.
	6	C	A		V97-0274, V97-0275	Controller may be blockaded when execute DP optimization with Zero Page Reclaim.	[Phenomena] (1) Controller may be blockaded with the following message, when execute DP optimization with Zero Page Reclaim. W0U0xy DMA error (DMA-y) (2) Unused capacity may not increase, when execute DP optimization with Zero Page Reclaim. <Equipment model / Firmware version> DF800S/M/H, V8.0/A(0880/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1)SA800, DF800S/M/H,DF800EXS/ES/EM/EH (2) I/F is Fibre Channel [Cause] (1) The maximum of a comparing table list is exceeded in error. (2) The zero data pages are not released in error. <Countermeasure> (1) The maximum value of DRR List is modified. (2) The zero data pages are correctly checked. <Action in the case of the failure> Phenomenon (1) 1) DP optimization is finished Please Reboot the array or replace the failed controller at dummy. After the controller is recovered, the other controller must be performed a dummy replacement. Please do not execute DP optimization with Zero Page Reclaim until the fixed firmware is applied. 2) DP optimization is not finished Please cancel DP optimization and replace the blockaded controller at dummy. After reboot the array or the controller is recovered, the other controller must be performed a dummy replacement. And please do not execute DP optimization with Zero Page Reclaim until the fixed firmware is applied. Phenomenon (2)
	7	C	B		V97-0267	Controller failure occurs when booting at iSCSI Boot	[Phenomena] Controller failure occurs with the following message when booting at iSCSI Boot. [DCTL]The PCI root complex error was detected[H0_IRQ6] <Equipment model / Firmware version> DF800S/M/H, V1.0/A(0810/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1)I/F is iSCSI (2) Initiator didn't ack the retransmitted packet and the retransmission timed out [Cause] In the condition of occurrence, fw buffer free condition is invalid and cause the recursive buffer free routine to go out of control. <Countermeasure> Replacing the buffer free routine from using recursive function call to a non-recursive function call <Action in the case of the failure> Dummy replace the failed controller . Please carry out a review of a course.

	8	C	B	SD3262240	V97-0271	Countermeasure for SATA HDD blockade, Enclosure failure, or Controller failure in mixed system of SATA HDDs and SAS HDDs	[Phenomena] SATA HDD, Enclosure in the additional unit, or Controller may blockade in mixed system <Equipment model / Firmware version> DF800S/M, V3.2/C(0832/C) or later DF800H, V4.0/A(0840/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] When the following conditions occurred at the same time, this phenomena may be appeared. 1) SAS HDDs and SATA HDDs are mixed in the system 2) Heavy work load (especially Write IOs) on SAS HDDs 3) Write IO to SATA HDDs 4) Using HGST SAS HDDs in the system (*)Model Name(Mounted HDD) DF-F800-AKH146(HGST HUS153014VLS300 / HUS156030VLS600) DF-F800-AKH300(HGST HUS153030VLS300 / HUS154530VLS300 / HUS156030VLS600) DF-F800-AKH450(HGST HUS154545VLS300 / HUS156045VLS600) [Cause] When many I/Os are issued to SAS HDDs and SATA HDDs, almost all Transmit Frame Buffers in SAS-Controller are in use by SAS HDDs access due to the firmware bug. SAS-Controller can't continue to send the upcoming data to SATA HDD(s) in this condition and SATA HDDs access timeouts may occur. The following failure may occur depend on the number of failed SATA HDDs or failed SATA HDDs position. - A SATA HDD blockade - Failure of Enclosure in the additional unit - Controller failure <Countermeasure> SAS-Controller will reserve a Transmit Frame Buffer to send upcoming SATA DATA not to occupy Transmit Frame Buffers for SATA HDD accesses. <Action in the case of the failure>	
	9	C	B		V97-0264	Enclosure incorrectly fails during backend diagnosis	[Phenomena] Enclosure incorrectly fails after indication two suspected failure parts during backend diagnosis. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.7/A(0897/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Backend diagnosis starts working when SES commands return [Cause] Firmware incorrectly detects enclosure failure after indicates two suspected failure parts during backend diagnosis in factor of enclosure error. <Countermeasure> When backend diagnosis works, firmware does not detect enclosure failure incorrectly. <Action in the case of the failure> After backend diagnosis indicates two suspected failure enclosures and ends without any failures occurring as shown below, if enclosure failure occurs with the message "Backend link error was detected", perform dummy replacement on the failed enclosure. Web message I5H000 Backend link error was detected(Unit-U,ENC-A) W0FA00 ENC alarm(Unit-U,ENC-A) :ENC/STR I5H401 The search for the failure part of backend route error ended(Path-X,Route-Y) W40000 Backend route warning has been detected(Path-X,Route-Y) :MANUAL/STR I5JD00 Suspected failure part has been detected(Unit-N,ENC-A) :ENC I5JD00 Suspected failure part has been detected(Unit-M,ENC-A) :ENC I5H301 The search for the failure part of backend route error started(Path-X,Route-Y)	

	10	C	B		HDS-107	Over 4Gbps bandwidth can not be specified for remote path on AMS2100 with H/W Revision 0200	[Phenomena] Over 4Gbps bandwidth can not be specified for remote path on AMS2100 with H/W Revision 0200 <Equipment model / Firmware version> DF800ES, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) TrueCopy or TrueCopy Extended Distance is enabled (2) Local array is AMS2100 with H/W Revision 0200 from which remote path is established (Doesn't matter what model the remote array is). (3) I/F is Fibre Channel [Cause] For AMS2100 with H/W Revision 0200, over 4Gbps bandwidth is wrongly rejected in the remote path setting, so over 4Gbps bandwidth can not be specified for remote path. (It is correct that over 4Gbps bandwidth can not be specified for remote path on AMS2100 with H/W Revision 0100, but for AMS2100 with H/W Revision 0200, over 4Gbps bandwidth is wrongly rejected) <Countermeasure> The maximum bandwidth for remote path is updated to 8Gbps for AMS2100 with H/W Revision 0200 <Action in the case of the failure> Please input a value between 100Mbps and 4Gbps for the bandwidth in the remote path setting on Hitachi Storage			
	11	C	B		V97-B024	TrueCopy(TC) pair status is changed to Failure for host I/Os when initial copy or resynchronization copy is in execution.	[Phenomena] TC pair status is changed to Failure with a following message when initial copy or resynchronization copy is in execution and TC pair's P-VOL receives host I/Os. Without array failure, it has a high likelihood of this trouble. WEB message : IB1T00 PSUE occurred[TrueCopy](LU-xxxxP/xxxxS) <Equipment model / Firmware version> DF800S/M/H, V9.3/A(0893/A) or later DF800ES/EM/EH, V9.3/A(0893/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) TC pair is created, resynchronized or swap [Cause] During initial copy and resynchronization copy, the area to copy is broken into small segments and each data transfer process copies a division. Whenever data transfer process finished copying a segment, two pointers, one for the starting address for the next data transfer process and the other for a boundary of dual write or not, are moved forward to the current position. When all data transfer are complete, both pointers are supposed to point at the end of LU. But when both P-VOL and S-VOL are DP-VOL, there is a case that the pointer for the boundary of dual write is not updated to the end of LU but point to the next to the last portion whose size is 10GB at max . If write command arrived to the last portion after the one data transfer process has reached the end of LU and before the pair status changes to Paired, although it should update both P-VOL and S-VOL, it only updates P-VOL and set on the differential bit, the double check routine to search differential data finds it and changes the pair status to Failure. <Countermeasure> The pointer to the boundary of dual write is updated to the end of LU when synchronizing copy is upon the completion of data			
	12	C	C		V97-B023	Controller failure occurs when connections are reconnected to a maximum of 255 hosts per port.	[Phenomena] Controller failure occurs with the following message when connections are reconnected to a maximum of 255 hosts per port. Microprogram error[ISM] <Equipment model / Firmware version> DF800S/M/H, V1.0/A(0810/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1)I/F board is iSCSI. (2)255 hosts are connected to each iSCSI Port. (3)255 Connections are closed and reconnected before issuing [Cause] There are no trigger to free the buffer when all 255 connections are closed and reconnected before the protocol chip return the completion of getting payload to the driver in login phase. <Countermeasure> Freeing the buffer by resetting the protocol chip. <Action in the case of the failure> .Dummy replace the failed controller. Please distribute the hosts to other iSCSI port and reduce the			
	V9.7/C, 0897/C							11/15/2010	285	None
V9.7/C 0897/C	1	N	-	-	V97-0270	Lower Drive Detach Threshold Mode support	Lower Drive Detach Threshold Mode support			

Base System V9.7/B, 0897/B	2	C	B	-	V97-S033	Countermeasure to the problem that ASIC time-out occurs in composition that mixed both iSCSI board and unpopulated board.	[Phenomena] ASIC time-out occurs in composition that mixed both iSCSI board and unpopulated board with one of following messages. (1)H203A0 DCTL time-out[H_PORT] (2)HD2100 Host transfer DMA error was over the threshold (3)H90320 Watch-dog time-out (4)HG0100 CTL communication send time-out (1) Controller failure when this issue occurs twice. Then please perform the action in the case of the failure. <Equipment model / Firmware version> DF800ES/EM, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) DF800ES/EM [Cause] When the data transfer in iSCSI Port is executed, it is necessary to check the presence of Error Detected Code. The hardware error is detected by mistaking the judgment of the presence of Error Detected Code at the data transfer by the cross I/O process when the I/F board is a unracking, and executing the data transfer start without Error Detected Code unjustified, and the controller is blockaded. <Countermeasure> The firmware refer to information of correct iSCSI I/F board side . <Action in the case of the failure> (1)Inhibit the load balance , and change the LU owner mapping to iSCSI Port from CTL with unpopulated board to CTL with iSCSI board.	
	3	C	B	-	V97-0280	Volume creation fails on the LUN with 2TB over.	[Phenomena] When a LUN is created with the size in the range from 2TB + 1 block to 2TB + 1024 blocks, volume create on the host side fails. <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) LUN is created with the size in the range from 2TB + 1 block (4,294,967,297 blocks) to 2TB + 1,024 blocks (4,294,968,320 blocks). Unified LUN corresponds to this condition too. (2) Volume creation on the host side is executed. The block [Cause] When DF800 receives the Read Capacity(10) command from host, then calculate the LUN size. If the LUN size is smaller than 2TB, DF800 returns the LBA with the real LUN size. If the LUN size is bigger than 2TB, DF800 returns the LBA with the value 0xFFFFFFFF. There is a firmware bug in the calculation process of LUN size. When the LUN size is in the range from 2TB + 1 block to 2TB + 1,024 blocks, DF800 judges incorrectly that LUN is smaller than 2TB, then DF800 returns LBA value incorrectly. <Countermeasure> Firmware is fixed to calculate the LUN size correctly. <Action in the case of the failure> Delete a LUN, and create a LUN with a smaller size than 2TB + 0 block (4,294,967,296 blocks) or with a bigger size than 2TB +	
	4	C	B	SD3355078	V97-0282	I/O performance degradation occurs in the start of RAID Manager(RM).	[Phenomena] Starting RM takes time while I/O performance degradation occurs. <Equipment model / Firmware version> DF800S/M/H, V3.2/A(0832/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Boot RM (2) Use HORCM LDEV to define pairs in the RM configuration [Cause] When RM starts, RM obtains host LU mapping information which includes Port Number and Host Group(HG) Number for each pair LU. This process checks every HG which can be defined for an array regardless of how many HGs are actually defined. This increases the number of necessary processes and cause a command response to take much time. <Countermeasure> When RM obtains host LU mapping information, only actually defined HGs are checked to improve command response time.	

	5	C	B	-	V97QA021	When transfer speed setting in Auto, there is the case that transfer speed display becomes mismatch.	[Phenomena] When transfer speed setting in Auto, there is the case that transfer speed display becomes mismatch. <Equipment model / Firmware version> DF800M/H/ES/EM/EH, V9.3/E(0893/E) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) DF800ES/EM or optional I/F board "DF-F800-DKF84" on DF800M/H/EH. (2) The channel speed setting of the FC port is "Auto". (3) Host reboot, PS OFF/ON, disconnect/connect a cable [Cause] When an auto-negotiation operated, the table setting value for the transfer rate display had been rewritten unjustified to due to the mistake of the judgment. To cause contradiction in an actual transfer rate and a set value of the table for the transfer rate display, the mistake was caused in the transfer rate display. <Countermeasure> The judgment of the transfer rate is corrected. <Action in the case of the failure> Because there is not a problem, a Linkup state please ignore.			
	6	C	C	-	V97-0284 V97-0285	Countermeasure for reporting the illegal Error Message when detecting failure in optional I/F.	[Phenomena] The controller failure may occur by Host DMA error when a certain failure occurs in optional I/F(I/F#1) in DF800ES/EM. HD21xy Host transfer DMA error was over the threshold (CTL-x, DMA-y) <Equipment model / Firmware version> DF800EM/ES, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1)DF800ES/EM (2)FC I/F or iSCSI I/F are installed as optional I/F. [Cause] There is a firmware bug about detecting a failure in optional I/F. This bug skips to detect the failure when a certain failure occurs in optional I/F. As a result, the illegal Error Message is reported and the controller failure occurs. <Countermeasure> The fix the firmware to detect the appropriate failure in the optional I/F(I/F#1). <Action in the case of the failure>			
	V9.7/H, 0897/H							2/8/2011	292	023
0897/H Base System V9.7/C 0897/C	1	I	-	SD3355078	-	Improvement in host response time during the start of RAID Manager	Improvement in host response time during the start of RAID Manager			
	2	I	-	-	-	Improvement of the simple trace (RASR0080)	The array serial number and the trace collected time are added to simple trace file name to make clear when and from what array a simple trace is collected. [New file naming convention of the simple trace] smpl_trc#_xxxxxxxx_yyyyyyyyyyyyy_0E.dat #　: CTL number on the Web connection side, xxxxxxxx　: serial number, yyyyyyyyyyyyy: Trace collected time			
	3	I	-	-	-	Host Group Option enhancement	"Unit Attention Change Mode" is supported.			
	4	I	-	-	-	Adjustment of time of link initialization at channel transfer speed "Auto" mode	Interval time of link initialization is changed to 100 milliseconds.			
	5	I	-	-	-	Improvement of the recovery time after a subsystem-down in DP configuration	Until this new firmware, DP pools which have no free capacity are formatted more preferentially. For this new firmware, in addition to such DP pools, DP pools which has no free capacity due to newly available capacity being consumed during format are also preferentially formatted.			

	6	C	A	-	V97-0290	Subsystem down may occur due to the remaining controller failure after another controller failure during heavy host I/O workload	[Phenomena] When a controller failure occurs by some cause in heavy I/O workload, the other controller may blockaded with the following WEB information message, which leads to subsystem down. HG0100 CTL communication send time-out <Equipment model / Firmware version> DF800H, V4.0/A(0840/A) and later DF800EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) DF800H or DF800EH (2) During heavy workload of host write access (3) Controller, which manages an LU receiving too many write, fails due some cause (4) There are more than 430 segments that have not been written to HDDs at the timing of (3). (5) The remaining controller checks the data consistency for the segments indicated in (4). (6) During (5), communication is issued from the Y core to the X core to check the response delay in host I/O. [Cause] There are cases where the remaining controller checks data consistency for data that has not been written to HDDs at the time of controller failure. It can take more than three seconds to check data consistency of over 430 segments. If the X core receives communication from the Y core at this timing, the problem occurs where the correspondence is interrupted wrongly until the data consistency check is complete. Due to this, "communication send time-out" occurs, the remaining controller fails, which leads to subsystem down. <Countermeasure> The firmware is modified to prevent the communication process from waiting more than three seconds during data consistency check by dividing the process when there are many numbers of segments. <Action in the case of the failure> Do the following procedures (1) and (2). (1) Turn PS OFF/ON (2) Replace the initially failed controller	
	7	C	A	-	V97-0315	When managing SnapShot or TruCopy Extended Distance (TCE) with Hitachi Dynamic Provisioning (HDP), Controller (CTL) Failure or Subsystem Down may occur.	[Phenomena] When managing SnapShot or TCE with HDP, the following phenomena may occur. (1) The SnapShot pair status is changed to "Failure" and CTL fails. The same phenomenon occurs in the other CTL, Subsystem Down occurs. (2) The P-VOL status of TCE pair is changed to "Failure" and CTL fails. The same phenomenon occurs in the other CTL, Subsystem Down occurs. (3) The S-VOL status of TCE pair is changed to "Inconsistent" and CTL fails. The same phenomenon occurs in the other CTL, Subsystem Down occurs. (4) CTL fails. The same phenomenon occurs in the other CTL, Subsystem Down occurs. [WEB information message] - In case of a controller blockade or subsystem-down HJ2CQU Microprogram error[POM] HJ2CQC Microprogram error[POM] - In case that SnapShot pair status is changed to "Failure" IB1S00 PSUE occurred[SnapShot](Data pool-XX) (XX: The number of Data Pool, which is used by the SnapShot pair with "Failure" status) - In case that TCE pair status is changed to "Failure" or "Inconsistent" IB1G00 Pair status changed by the error(CTG-YY) (YY: The number of CTG, which is used by the TCE pair with "Failure" or "Inconsistent" status)	

							[Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Dynamic Provisioning is enabled. (2) Copy-on-write SnapShot or TrueCopy Extended Distance is enabled. (3) There is virtual LU in the data pool. (4) The capacity of a virtual LU of (3) is 3,302,976KB (about 3.2GB) or more. (5) One of the following operations or situation. -Resync, restore, or remove the SnapShot pair with old data evacuated. -Write to the SnapShot P-VOL or S-VOL with "Split" status. -Resync, split, remove, or swap the TCE pair. -Write to the TCE P-VOL or S-VOL. -The SnapShot pair status is changed to "Failure". [Cause] When evacuated old data becomes unnecessary, the management table deletion process is executed. There is firmware bug in correspondence checking logic of this process for virtual LU in the data pool. When management table is divided, illegal NG in correspondence check and CTL failure occurs with the operation or situation enumerated in Conditions of Occurrence (3). When the same phenomenon occurs in another CTL, Subsystem Down occurs. <Countermeasure> Fix firmware bug in correspondence checking logic of this process
	8	C	A	-	V97-0308	When the failures occur in all battery units during host I/O, subsystem hang-up may occur.	[Phenomena] When the failures occur with the following WEB information message in all battery units during host I/O for the LU of RAID1/RAID1+0 of SATA HDD, HDD Write processes may stop and subsystem hang-up may occur. One of the following WEB information messages is displayed. W03z0x Battery alarm(Battery-x) W01z0x CTL alarm (CTL-x) W08zy0 PS alarm (CTL-Unit,PS-x) W0400x Battery backup circuit alarm(CTL-x) W0Hz0x UPS alarm (UPS-x) <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) SATA HDD (2) RAID1 or RAID1+0 (3) There are two or more LUs in the RAID group of (2). (4) Host I/Os (5) One of the following failures of no active battery units occurs. - When the forced write through mode of the system parameter is valid, a blockade of the Control Unit (it is not this condition in the single controller configuration), a power unit failure or UPS [Cause] When subsystem has no active battery units during host I/Os, the firmware aborts currently-running HDD Write processes and performs the special HDD Write process which writes the dirty data first. When an HDD Write process for two or more LUs of SATA RAID1 or SATA RAID1+0 is aborted, this process may neglect the abort request. In that case, the abort request is repeated and subsystem hang-up occurs. <Countermeasure> The firmware correctly aborts the HDD Write processes. <Action in the case of the failure> Turn PS OFF/ON.

	9	C	B	SD3353803	V97-0288(1)	After executing the Volume Migration, the Load Balancing does not run. Or, Load Balancing can not be worked evenly between the controllers or cores.	[Phenomena] After executing the Volume Migration, the following phenomena occur. (a) The Load Balancing does not run. (b) The Load Balancing can not be worked evenly between the controllers or cores. <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) The Load Balncing is set "Enable". (default: Enable) Storage Navigator Modular2 (GUI) [Performance]-[Tuning Parameter]-[System tuning]-[Load Balancing] (2) The Modular Volume Migration is locked off and enable. (3) After executing the Volume Migration, each of the following event occur. In case of phenomena (a) - One of the target LUs of the Volume Migration is deleted. - Each target LU of the Volume Migration exists in the different controller or core. In case of phenomena (b) - Both of the target LUs of the Volume Migration exist in the same controller or core. [Cause] In the Load Balancing, the target LU whose ownership is changed is selected based on the I/O load information.The performance Information is kept tabs on by the internal LUN. But the number of Cache Hit read Commands which is one of the performance information was kept tabs on by the middle LUN wrongly. As a result, following events occur. In case one of the target LUs of the Volume Migration is deleted, the Load Balancing refers the information of deleted LU and determines the change of ownership is unnecessary. In case each target LU of the Volume Migration exists in the different controller or core, the Load Balancing can determine the change of ownership is unnecessary because ownership of LU recieved I/O load is other controller or core. Also, in case both of the target LUs of the Volume Migration exist in the same controller or core, the Load Balancing executes uneven I/O load balancing because that keeps tabs on the number of Cache Hit Read Commands in the LUN which do not recieved I/O load. <Countermeasure> The processing which counts the number of Cache Hit Read Commands is done in the internal LUN. <Action in the case of the failure> Follow the procedures below. (1) Set the Load Balancing "Disable".	
	10	C	B	EUC1291668	V97-0302(1)	Controller failure may occur in heavy workload under TrueCopy Extended Distance (TCED) configration	[Phenomena] Controller failure may occur with following WEB information message in heavy workload under TCED configration WEB information message : HGA400 Data pool wait time-out <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) TCED copies work under TCED configuration (2) Cache segments are exhausted due to heavy workload caused by copy of TCED or host I/Os (3) The Persistent Reserve or reset command is received [Cause] When cache segments are depleted because host I/O or copy operations work in heavy workload in TCED, if internal exclusion for data copy stops or switchs by receving the Persistent Reserve command or reset command, the data copy wrongly continues. As a result, time-out for exclusive resources (Data pool wait time-out) occurs, which causes a controller failure. <Countermeasure> The firmware is modified so that data copy will not continue inappropriately. <Action in the case of the failure> Recover the failed controller by dummy-replacement. Or adjust the TCED configuration by reducing the number of pairs to improve the heavy workload.	

	11	C	B	SD3420606	V97-0311	When the link error that is intermittent occurred on Fibre Channel Link in executing host I/O, following WEB information message is displayed, and controller blockade. WEB information message : HB0A0x H-FPC hardware error(Port-x)	[Phenomena] When the link error that is intermittent occurred on Fibre Channel Link in executing host I/O, following WEB information message is displayed, and controller blockade. One of the following WEB information messages is displayed. HB0A0x H-FPC hardware error(Port-x) or W3Rxyz Interface Board alarm(CTL-w,I/F-z) or HF0100 Data transfer check error[SEGPOSERR] or W1K00x Data transfer check error[SEGPOSERR](CTL-x) or H20100 Parity generation LA error[DRR] or W0N00x Parity generation LA error[DRR](CTL-x) or H203A0 DCTL time-out[H_PORT] <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.3/A(0893/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Fibre Channel I/F (2) Executing host IO. (3) LinkService command is received. (4) By causes such as Fibre Channel cable deterioration and higher host side SFP trouble or interface board trouble of an array device, the link error that is intermittent occurred on Fibre Channel Link in executing host I/O. (5)The host write data transfer error occurs because of '(4)', and the check condition "0B/4B00" response is generated. [Cause] When the check condition "0B/4B00" responds detecting the Link error when LinkService system command is executed, the operation stop is directed to Fibre I/F Chip once. When the errorIdle signal is accepted in this, Fibre I/F Chip might be operated unjustified. Therefore, Fibre I/F Chip malfunctions. <Countermeasure> When error Idle signal is accepted, doesn't begin to operate unjustified Fibre I/F Chip. <Action in the case of the failure> Dummy replacement of the failed controller	
	12	C	B	EUC1303162	V97-0316	When recovering TrueCopy path, path status stagnates in "Diagnosing" and does not recover.	[Phenomena] When recovering TrueCopy path, path status stagnates in "Diagnosing" and does not recover. <Equipment model / Firmware version> (Phenomena(1)) DF800S/M/H/ES/EM/EH, V9.0/A(0890/A) and later (Phenomena(2)) DF800S/M, V3.2/A(0832/A) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. - Phenomenon (1) (1) The remote array is DF800S/EXS/M. (2) I/F type of remote array is "FC" and the port number is one of 1A/1B (DF800S/EXS) or 1A/1B/1C/1D (DF800M). (3) The local array and the remote array are connected through FC-Switch. (4) Path failure, which not recovers automatically, occurs. (5) Operate "recover path" manually. - Phenomenon (2) (1) Path failure, which not recovers automatically, occurs. (2) The local array and the remote array are connected through FC-Switch. (3) The remote array is detached from FC-Switch.	

							[Cause] When path failure, which not recovers automatically, occurs and "Recover path" is performed manually, there is firmware bug in logic of checking status of remote array connection. Illegal status is reported and path status stagnates in "Diagnosing".(Phenomena (2)) Process of recovering path stops illegally, path status stagnates in "Diagnosing".(Phenomena (1)) <Countermeasure> Fix firmware bug in logic of checking status of remote array connection. Add retrying to process of recovering path aiming no stopping illegally. <Action in the case of the failure - Phenomenon (1)> Reboot array or do the following procedures (1) and (2). (1) Split TrueCopy pair, delete each path of this pair, and re-create remote path. (2) Resync TrueCopy pair. <Action in the case of the failure - Phenomenon (2)> Do the following procedures. (1) Reconnect remote array. (2) Reboot array or do the following procedures (3) and (4). (3) Split TrueCopy pair, delete each path of this pair, and re-create remote path. (4) Resync TrueCopy pair.
	13	C	B	-	V97-0310 (same as DF700-0296)	A controller blockade may occur when host I/Os are issued with the queue depth which is equal to or more than 625 to a frontend port.	[Phenomena] A controller blockade may occur with the following WEB information message when host I/Os are issued with the queue depth (*1) which is equal to or more than 625 to a frontend port. When this problem occurs in both controllers, Subsystem-down occurs. WEB information message: HB0A0y H-FPC hardware error(Port-y) (*1) When host I/Os are issued with the queue depth which is more than 512 to a frontend port, the following WEB information message is displayed. WEB information message: I6GE00 [Performance]Queue-full occurs often(Port-xy,Connected host num.=zzz,Queue depth=512) <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Fibre Channel I/F (2) Host I/Os are issued with the queue depth which is equal to or more than 625 to a frontend port. (The number of queue depth of a frontend port is 512.) [Cause] Due to the firmware bug in the process for a command reset frame (*2) during the heavy queue-full condition When a command reset frame (*2) is received, the firmware should stop host I/O processes and discard host I/Os which are required to be reset. But, when all of the conditions of occurrence are met, host I/O processes do not be stopped due to a firmware bug. And, host I/Os which are required to be reset may be performed before the firmware discards these I/Os. A controller blockade occurs at that time. (*2) Command reset frame: PLOGI, LOGO, Logical Unit Reset, Target Reset and TPRLO <Countermeasure> When all of the conditions of occurrence are met, the firmware certainly stops host I/O processes. <Action in the case of the failure> Perform the procedures (1) to (2). (1) Set the number of the total queue depth of hosts or HBAs to 512 or less for a frontend port. (2) Perform the dummy replacement of the blocked controller.

	14	C	B	-	V97-B025	When the host is rebooted in host I/O in iSCSI maximum host connection (255) composition, a controller blockaed. and following WEB information message is displayed.	[Phenomena] When the host is rebooted in host I/O in iSCSI maximum host connection (255) composition, a controller blockaed. and following WEB information message is displayed. WEB information message : HH7Exy Microprogram error[ILM] <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) iSCSI I/F (2) iSCSI maximum host connection (255) composition (3) 255 connections close at the same time by host rebooting simultaneously. [Cause] The reset instruction command is done to execute the reset processing in all cores when the connection closes and the queuing is done to another core.When 255 reset instructions are generated at the same time, the instruction command queue might become a queue full . However, the controller blockage is generated misjudging a queue full to be abnormal by the trouble of the queue full check by the reset processing. <Countermeasure> Prior of a queue full is checked before the queuing is done to the instruction command queue.After being able to become empty an instruction command queue when the instruction command cue is a queue full, the queuing does the reset instruction command. <Action in the case of the failure> Dummy replacement of the failed controller	
	15	C	B	-	V97-0289	When an intermittent failure occurs in an iSCSI interface during heavy host I/O workload, a controller blockade may occur.	[Phenomena] When an intermittent failure occurs in an iSCSI interface during heavy host I/O workload, controller blockade may occur in resetting the iSCSI protocol chip with the following WEB information message. WEB information message : HD2400 DRR time-out <Equipment model / Firmware version> DF800S/M/H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1)iSCSI I/F (2)Resetting the iSCSI protocol chip (3)Internal queue-full is occured by heavy I/O condtion. [Cause] When the firmware detect the failure of iSCSI protocol chip and reset the chip in condition that the internal queue is full by heavy I/O, firmware inhibit the interrupt vector incorrectly in resetting process .The interrupt processing timeout will be occured as a result. <Countermeasure> The firmware unlock the interrupt in resetting process. <Action in the case of the failure> Dummy replacement of the failed controller	
	16	C	B	-	V97-0317	When continuous media errors of HDD occur, I/O performance degradation may occur.	[Phenomena] When continuous media errors of HDD occur permanently in host I/O, I/O performance degradation may occur. <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Media errors of HDD occur in Host I/O. (2) After Media error recovery, same errors occur permanently.	

							[Cause] When same errors occur after Media error recovery, the firmware tries to blockade an error HDD as soon as possible. But, the firmware cannot blockade the error HDD due to a firmware bug. Therefore host I/O performance is slow down because of the error HDD recovery many times. <Countermeasure> Whether the same error occurred after HDD's reassign is correctly judged. <Action in the case of the failure> Apply the fixed firmware.	
	17	C	B	-	V97-0301	Controller may be blockaded when Enclosure in RKAK failure occurs.	[Phenomena] When failures occur on Enclosure in RKAK that is connected to Controller direct, the Controller may be blockaded with following Web information message. WEB information message : H30L00 Backend error count of the CTL was over the threshold[SAS_FW REBOOT NG](CTL-x) <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. - In case of DF800H/DF800EH (1) Two or more RKAKs are connected to Control unit. (2)Intermittent failures occur on the following either parts when booting system or during I/O operations. (Unit-1, ENC-0) (Unit-1, ENC-1) (Unit-2, ENC-0) (Unit-2, ENC-1) (Unit-3, ENC-0) (Unit-3, ENC-1) Enclosure cable connected to CTL-0 and Unit-1, ENC-0 Enclosure cable connected to CTL-1 and Unit-1, ENC-1 [Cause] When failures on backend route occur, Controller resets the backend to recover the failure during system booting or I/O operations. If failures occur on Enclosure or Enclosure cable during reset of backend, firmware may wrongly detect the Controller failure. <Countermeasure> Firmware correctly detects the failure part during reset of backend. <Action in the case of the failure> The case Controller blockade occurs with following Web information message, and after replacing the Controller, Controller blockade occurs again with similar message, replace Enclosures and Enclosure cables connected to Controller direct. WEB information message : H30L00 Backend error count of the	
	18	C	B	-	V97-0307	When failures occur on backend route, firmware may incorrectly indicate suspected failure part.	[Phenomena] Even if failure part is ENC or HDD, CTL is detected as suspected failure part on backend diagnosis. There is a possibility of displaying following WEB information message. I5H4AB The search for the failure part of backend route error ended (Path-x, Route-y) W40000 Backend route warning has been detected (Path-x, Route-y) I5JDe0 Suspected failure part has been detected (Unit-x, ENC-z) I5JCzx Suspected failure part has been detected (CTL-x) I5H3AB The search for the failure part of backend route error started (Path-x, Route-y) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.7/A(0897/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. - In case of DF800H/DF800EH (1)Five or more RKAKs are connected. (2)Failures on HDD or ENC occur during Read I/O to HDD. (3)The failure part can not be detect in backend diagnosis, and suspected failure parts are displayed on Web information message. - In case of DF800S/DF800M/DF800ES/DF800EM (1)Two or more RKAKs are connected.	

							[Cause] Firmware judges the suspected failure part by counting the increase of hard error counters. An increase of controller's hard error counter may be illegally detected when backend route failure occurs during Read I/O to HDD. Hard error counters illegally up on CTL and ENC connected to CTL directly. And firmware incorrectly judges the suspected failure part. <Countermeasure> Firmware does not detect illegally increase of hard error counters. <Action in the case of the failure> There is a possibility of displaying following WEB information message. Replace CTL and ENC displayed. If similar message is displayed again, apply the fixed firmware. I5H4AB The search for the failure part of backend route error ended (Path-x, Route-y) W40000 Backend route warning has been detected (Path-x, Route-y) I5JDe0 Suspected failure part has been detected (Unit-x, ENC-z) I5JCzx Suspected failure part has been detected (CTL-x) I5H3AB The search for the failure part of backend route error started (Path-x, Route-y)	
	19	C	B	-	V97-0295	I/O performance degradation may occur when a SATA HDD is blockaded or removed and then a failure occurs in the slot of the blockaded HDD.	[Phenomena] I/O performance degradation may occur when a SATA HDD is blockaded or removed with the following WEB information message and then a failure occurs in the slot of the blockaded HDD. WEB information message : W09zab HDU alarm (Unit-x, HDU-y, Type-c) <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1)I/O is issued to SATA LU. (2)SATA HDD is removed or blockaded. (3)Connection closing process of SATA HDD is executed after (2). (4)After (2), a reset command is issued to SATA HDD because of IO error. (5)(3) and (4) are generated at the same time. (6)Failures occur on the slot that the SATA HDD installed [Cause] Firmware does not work connection closing process when SATA HDD reset is executed. So if failures occur on the slot that the SATA HDD installed, firmware receive temporarily interrupts from the slot. and then firmware stop the I/O from the route and search the part that issue interrupts. Backend I/O performance is slow down when this situation continues. <Countermeasure> SATA HDD remove from system when reset and connection closing process are executed at the same time. <Action in the case of the failure> In the case to remove HDD, mount exchanged HDD. Replace the blockade HDD.	

	20	C	B	-	V97-0298(1) (same as DF700-0292)	For TrueCopy (TC) - ShadowImage (SI) cascade configuration, TC pair creation is wrongly performed with a SI pair in Failure (S-VOL Switch)(for Hitachi Storage Navigator Modular2 (HSNM2)).	[Phenomena] While a TC pair is being created with P-VOL of SI as P-VOL of TC, even if a double drive failure (triple drive failure for RAID6) occurs on the SI P-VOL and it causes SI pair status to change to Failure (S-VOL Switch)(for HSNM2), the TC pair creation is wrongly performed. And then TC pair status changes to Failure(for HSNM2) soon. The message to be displayed when LU failure occurs on the SI P-VOL: W0Q000 LU alarm <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) SI is enabled. (2) TC is enabled. (3) SI I/O Switch Mode is enabled. (4) The pair status of the SI pair is Paired(for HSNM2). (5) A double drive failure (triple drive failure for RAID6) occurs on the SI P-VOL at the same time a TC pair creation is specified with P-VOL of SI as P-VOL of TC. [Cause] At the time of TC pair creation, SI pair status is preliminarily checked to see if its pair status is appropriate for SI - TC configuration. When a drive failure occurs shortly after this preliminary check, the SI pair status wrongly changes to Failure(S-VOL Switch). Since the preliminary check is already complete, even if the SI pair status is Failure(S-VOL Switch), the TC pair creation with the SI P-VOL in Failure(S-VOL Switch) keeps on and finally finishes. <Countermeasure> To prevent TC pair creation from being performed wrongly, mutual exclusion is made in the time between the preliminary check of SI pair status and completion of TC pair creation so the SI pair status does not change during that time <Action in the case of the failure> Do the following procedures (1) to (3). (1) Release the TC pair. (2) Perform the recovery procedure for the SI I/O switch function (3) Create the TC pair again.	
	21	C	B	-	V97-0298(2) (same as DF700-0293)	When a drive failure occurs during SnapShot (SS) restore operation, a controller failure may occur or the pair status changes to PAIR without performing actual restore copy.	[Phenomena] When one of the failures described below (*1) occurs on the P-VOL or data pool at the same time SS restore operation is specified, the following phenomena may occur. (Phenomenon A) When a SS P-VOL has relationships with a V-VOL, the pair status changes to PSUE and then a controller failure may occur with the following message. WEB information message: HJ2Dxx Microprogram error [SNR] (Phenomenon B) When a SS P-VOL has relationships with multiple V-VOLs, the SS pair specified for restore operation does not change to PSUE status but to PAIR status without performing actual restore copy. (*1)Drive failures - PIN over : "PIN is over *******" - LU failure :"W0Q000 LU alarm" - Double drive failure (triple drive failure for RAID6): "I301xy HDU error(Unit-X, HDU-Y)" <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later	

							[Cause] At the time of SS restore operation, because the preliminary pair status check process and transition process for PSUE do not make mutual exclusion, if a drive failure occurs after SS restore operation is specified, the pair status wrongly changes from PSUE to COPY, which can cause a controller failure or allow the pair status to change to PAIR without performing actual restore copy. <Countermeasure> The preliminary pair status check process and transition process for PSUE make mutual exclusion and if the pair status is confirmed PSUE, the restore operation will not be executed. <Action in the case of the failure> Release all pairs related to the P-VOL and then perform a recovery procedure for each problem occurring. After this, restore backup data of the V-VOL to an LU that is intended to be a P-VOL and then specify pair creation to the LU.	
	22	C	B	-	V97-0288(2)	Even though the Load Balancing is enabled, I/O load may not improve between controllers or cores.	[Phenomena] Even though the Load Balancing is enabled, I/O load may not improve between controllers or cores. <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) The Load Balncing is set "Enable". (default: Enable) (2) Read Command is issued from the host. [Cause] The performance information which the Load Balancing keeps tabs on is below. - The number of Cache Hit Read Commands - The number of Cache Miss Read Commands - The number of Write Commands - The number of Cross-call Commands In case Read Command hits the cache, the Load balancing counts "the number of Cache Hit Read Commands". But in addition, that also counts "the number of Cache Miss Read Command" wrongly. Because the Load Balancing selects the target LU whose ownership is changed based on the wrong information, I/O load may not improve after changing the LU ownership by the Load balancing. <Countermeasure> In case Read Command hits the cache, the Load Balancing counts only "the number of Cache Hit Read Commands". <Action in the case of the failure> Follow the procedures below. (1) Set the Load Balancing "Disable". Storage Navigator Modular2 (GUI) [Performance]-[Tuning Parameter]-[System tuning]-[Load Balancing] (2) After that, change the LU ownership manually and equalize I/O load between the cores.	
	23	C	B	-	V97-0293	When a permanent DMA transfer error occurs during host I/Os, a check condition response for a host I/O or host command time-out may occur repetitively without a controller blockade.	[Phenomena] When a permanent DMA transfer error occurs in an HDD Write during host I/Os, the following phenomena may occur repetitively without a controller blockade. - A host detects a command time-out. - The check condition "0B/C000" is send for a host read command. - The check condition "0B/C006" is send for a host write command. <Equipment model / Firmware version> DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) the controller of "H/W Rev.0200" (2) Host I/Os (3) A permanent DMA transfer error occurs in an HDD Write.	

							[Cause] When a DMA transfer error occurs in an HDD Write, the firmware checks and terminates this error DMA transfer. Then the firmware retries other DMA transfer. But the firmware always judges that the transfer number of an error DMA transfer is zero incorrectly. So, when the transfer number of an error DMA transfer is not zero, the firmware cannot block the controller and the DMA transfer error occurs repetitively, because the firmware retries the error DMA transfer. As a result, an I/O job detects job time-out and sends the check condition response. Or host detects command time-out. <Countermeasure> The firmware correctly checks the error DMA transfer #. <Action in the case of the failure> Apply the fixed firmware.		
	24	C	B	-	V97QA029	A controller blockade may occur during highly-loaded host I/Os for the LU of RAID1 or RAID1+0 of SATA HDDs.	[Phenomena] A controller blockade may occur with the following WEB information message during highly-loaded host I/Os for the LU of RAID1 or RAID1+0 of SATA HDDs. WEB information message : "HZ0N0x Kernel processing error (CTL-x)" <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) SATA HDD Or a data recovery process (dynamic sparing, correction copy or copy back) is performed in the kind of HDDs other than SATA HDD. (2) LU of RAID1 or RAID1+0 (3) HDD Write process tries to write intensively more data to one HDD at a time due to performance improvement. (4) highly-loaded host I/Os (5) no free cache segment [Cause] HDD Write process searches a free cache segment for a target HDD. But HDD Write process incorrectly continues to search a free cache segment even if there are no free cache segments for a target HDD. When HDD Write process has a huge amount of data for a target HDD, a search process time-out occurs and a controller blockade occurs. <Countermeasure> HDD Write process searches a free cache segment for a target HDD. But HDD Write process incorrectly continues to search a free cache segment even if there are no free cache segments for a target HDD. When HDD Write process has a huge amount of data for a target HDD, a search process time-out occurs and a controller blockade occurs.		
	25	C	B	-	V97-0300	When SSD addition or SSD replacement is performed during subsystem online, "Vendor ID" of the installed SSD cannot be displayed in Storage Navigator Modular2 or WEB.	[Phenomena] When SSD addition or SSD replacement is performed during subsystem online, all of the following phenomena occur. - "Vendor ID" of the installed SSD cannot be displayed in Storage Navigator Modular2 or WEB. Storage Navigator Modular2 : [Components]-[Trays]-[Tray xy]-[HDU xy]-[Properties]-[Vendor ID] WEB : [http://IP address/drvfirm]-[Drive Information]-[Vendor ID] - "Vendor ID" of the blocked SSD cannot be written in a E-mail of E-mail Alert Function. - Automatic drive firmware download process cannot be performed even if the HDD firmware version of the installed SSD is older than the one which the firmware of subsystem has. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.7/A(0897/A) and later [Conditions of Occurrence] The problem occurs certainly when the following condition is met. SSD addition or SSD replacement is performed during subsystem online.		

							[Cause] When the firmware detects a installed HDD, the firmware issued inquiry command to the HDD before and after a spin-up of HDD and gets Vendor ID. But, when HDD kind of a detected HDD is SSD, the firmware incorrectly initializes Vendor ID information of this SSD in a inquiry command process after a spin-up of HDD. <Countermeasure> The firmware incorrectly initializes Vendor ID information. <Action in the case of the failure> Turn PS OFF/ON.	
	26	C	C	-	V97-0297(1)	Incorrect information may be displayed when using a RAID Manager (RM) command to confirm the configuration on the array and host	[Phenomena] Some of the LUs may not be displayed when using the raidscan command in RM to confirm the configuration on the array and host. <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. Incorrect information by the raidscan command appears in the following three conditions. - In combination of Modular Volume Migration (MVM) and LU deletion (1) An LU(a) is created with the maximum LUN for the array. (2) MVM is performed on LU(a) and LU(b) which is another LU (3) The LU(b) is deleted (4) The raidscan command is executed - In combination of MVM and unifying LU (1) An LU(a) is created with the maximum LUN for the array. (2) MVM is performed on LU(a) and LU(b) which is another LU (3) The LU(b) (as the child) is unified into the LU(a) "as the parent" (4) The raidscan command is executed [Cause] The raidscan command searches all existing LUs to the LU with the maximum LUN to display configuration information. Because LUs to be displayed are wrongly determined by referring not to the internal LUNs but to the middle LUNs, The information of some LUs is not displayed. <Countermeasure> The firmware is modified so the raidscan command will refer to middle LUNs. <Action in the case of the failure> Execute the raidscan command with the"-p <port> [hgrp]" option for determining host groups.	
	27	C	C	-	V97-0297(2)	Incorrect information may be displayed when using a RAID Manager (RM) command to confirm data pool status	[Phenomena] Incorrect LUNs may be displayed when using the pairdisplay command with " -v pid" option in RM to confirm data pool status. <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. Incorrect information by the pairdisplay command appears in the following two conditions. - Using Modular Volume Migration (MVM) (1) The LU which on MVM is performed is specified to a data pool (2) Data pool information is displayed by the pairdisplay command with "-v pid" option - Using Dynamic Provisioning (DP) (1) A DP pool is created (2) An LU(a) is created with the maximum LUN for the array. (3) The LU(a) is specified to a data pool (4) Data pool information is displayed by the pairdisplay command with "-v pid" option	

							[Cause] The pairdisplay command with the -v pid option displays data pool status. It wrongly displays internal LUN instead of the middle LUN. <Countermeasure> The firmware is modified so that the pairdisplay command will refer to middle LUNs. <Action in the case of the failure> Refer to data pool information on the Hitachi Storage Navigator Modular2.
	28	C	C	-	V97-0296	Invalid "LOADB" TRACE information may be displayed in TDCONV4.	[Phenomena] Invalid LU performance information may be displayed for 123 lines at one time in "LOADB" TRACE of the following sheet of TDCONV4. The sheets of TDCONV4 : "CTL0_ALL", "CTL0_ALL_Y", "CTL1_ALL" or "CTL1_ALL_Y" <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem occurs certainly when all of the following conditions are met. (1) Problem ID V97-0288(1) occurs. (2) Load Balancing function is performed due to highly-loaded host I/Os. [Cause] When Load Balancing function performs a LU ownership change process, LU performance information is written to "LOADB" TRACE. But, when Load Balancing function does not perform a LU ownership change process, the number of LU performance information which is written to "LOADB" TRACE incorrectly is set to 123. So, invalid LU performance information is displayed for 123 lines at one time. <Countermeasure> When Load Balancing function does not perform a LU ownership change process, Load Balancing function sets the number of LU performance information which is written to "LOADB" TRACE to zero correctly. <Action in the case of the failure> Apply the fixed firmware.
	29	C	A	EUC1291668	V97-0302(2)	Host I/Os may stop under heavy workload in TrueCopy Extended Distance (TCED) configuration.	[Phenomena] When host I/O workload is heavy in TCED configuration, write operations to the HDDs receiving the I/Os may not work, then host I/Os for the LU may stop. <Equipment model / Firmware version> DF800S/M/H, V8.0/A(0880/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) TCED copies work under TCED configuration. (2) Cache segments are exhausted due to heavy workload caused by copy of TCED or host I/Os [Cause] When copy operation of TCED works in heavy workload, the firmware wrongly does not release cache segments which the array uses during the copy operation. So, when cache segments are depleted, all processes for the LU do not work, and then write access to the HDDs stops, though read or write processes to the other LUs can still work. <Countermeasure> The firmware is modified so that the depletion of cache segments will not continue by modifying the release judgment of the segment. <Action in the case of the failure> Turn PS OFF/ON.

	30	C	A	-	V97-B028	When many host groups or iSCSI targets are deleted at the same time, two controller failures may occur and subsystem-down occurs.	[Phenomena] When many host groups or iSCSI targets are deleted at the same time, two controller failures may occur with the following WEB information message and subsystem-down occurs. H90320 Watch-dog time-out <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) LU is mapped in a host group or iSCSI target. (2) There are host groups or iSCSI targets more than 80. (3) 80 or more host groups/iSCSI targets are deleted at the same time. [Cause] When host groups or iSCSI targets are deleted, the management information of all host groups/iSCSI targets is incorrectly copied between a cache memory and a local memory every time the management information of one host group/iSCSI target is updated. So, when 80 or more host groups/iSCSI targets are deleted at the same time, a time-out of the deletion process may occur. In this case, two controller failures occur and subsystem-down occurs. <Countermeasure> The management information of all host groups/iSCSI targets is updated and then copied between a cache memory and a local memory. <Action in the case of the failure> Turn PS OFF/ON.			
	31	C	B	-	V97-0314	When an HDU blockade or an ENC blockade occurs, a controller failure may also occur.	[Phenomena] When an HDU blockade or an ENC blockade occurs, a controller failure may also occur with the following WEB information message. One of the following WEB information messages is displayed. HZ0N0x Kernel processing error HG0312 Resource release time-out <Equipment model / Firmware version> DF800S/M/H, V6.5/A(0865/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Dual controllers (2) A failure occurs where both controllers cannot detect an HDU or an ENC. (3) Both controllers try to perform a blockade process at the same time after (2). [Cause] A communication process between both controllers is performed in an Alarm LED lighting process after an HDU blockade or an ENC blockade. But, A communication process between both controllers is incorrectly rejected during an Alarm LED lighting process. So, a time-out of the communication process between both controllers may occur. In this case, a controller failure occurs. <Countermeasure> A communication process between both controllers can be performed during an Alarm LED lighting process. <Action in the case of the failure> dummy replacement of the blocked controller			
	V10.0/A, 08A0/A							1/14/2011	295	None
V10.0/A 08A0/A Base System V9.7/H, 0897/H	1	N	-	-	-	SAS 7.2K HDD support	SAS 7.2K HDD (2TB) is supported.			
	2	N	-	-	-	Self Encryption HDD (SED) and new program product Data At Rest Encrypting support	SED HDD (600GB) and new program product Data At Rest Encrypting are supported.			
	3	N	-	-	-	Dynamic Provisioning enhancement	Full Capacity Mode is supported.			
	4	I	-	SD3330611	-	Improvement for CPU utilization reduction on Dynamic Provisioning	In the Dynamic Provisioning environment, the checking overhead of the all RAID group status is improved, so that the CPU utilization will be reduced.			
	5	I	-	-	-	Improvement for Mapping Guard	The setting change of the Mapping Guard is changed so that it was applied only to defined LUN.			

	6	C	-	SD3357545	VA0-0141	The incorrect WEB message is displayed when the HDU type is changed in the Dense tray.	[Phenomena] When the HDU type of the Dense tray is changed according to a procedure not correct, the incorrect WEB message is displayed. [Correct WEB message] I30D00 The several different types of disk drives are installed in the RKAKX(Unit-xx,HDU-yy) [Incorrect WEB message] W09AZZ HDU alarm(Unit-xx,HDU-yy,Type-Unknown) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.5/A(0895/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Pull out one or more SATA HDDs from Dense tray which is installed only SATA HDDs (2) Insert the SAS 7.2K HDDs into the slots that HDD is pulled out in procedure (1) (3) SAS 7.2K HDDs that are inserted in procedure (2) blockade (4) Turn PS OFF/ON			
							[Cause] Because the HDU information that is managed by firmware became to be wrong status, the incorrect WEB message was displayed. <Countermeasure> Firmware is modified as guard logic so that the incorrect WEB message doesn't be displayed. <Action in the case of the failure> Ignore the message "W09AZZ", and take an action according to the other WEB messages such as "I30D00".			
	V10.0/B, 08A0/B							6/24/2011	308	None
V10.0/B 08A0/B Base System V10.0/A, 08A0/A	1	I	-	-	-	Improvement for restoring Master Authentication Key of SED	When restoring Master Authentication Key of SED from a backup file, the product number of array and ID of the Key in the file are checked by the array not to restore from wrong files.			
	2	I	-	-	-	Improvement for firmware downgrade of SED	When Data At Rest Encryption is installed and enabled, the firmware downgrade is not allowed.			
	3	I	-	-	-	Improvement for Full Capacity Mode on Dynamic Provisioning	Improvement of guarding to make DP-VOL of Full Capacity Mode or change Full Capacity Mode when causing the depletion			
	4	C	A	EUC1309008	VA0-0182	Access lost may occur during host random write commands, because a lot of dirty data cannot be processed on a cache memory.	[Phenomena] I/O performance degradation may occur during host random write commands, because a lot of dirty data cannot be processed on a cache memory and there are no available cache segments. Finally, host access lost may occur. <Equipment model / Firmware version> DF800S/M/H, V3.0/A(0830/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) The following number of HDDs is installed. -DF800S/ES: 17 HDDs and more -DF800M/EM: 25 HDDs and more -DF800H/EH: 33 HDDs and more (2) There are more than one RAID Groups in the array. (3) One of the following conditions ((3-1), (3-2) and (3-3)) is met. (3-1) Cache Partition Manager is disabled. There are two RAID Groups in the array. The number of "Dirty Data Stop Opportunity" is set to 16% and over. (The default number of "Dirty Data Stop Opportunity" is 5%.) (3-2) Cache Partition Manager is disabled. There are more than two RAID Groups in the array. The number of "Dirty Data Stop Opportunity" is set to 11% and over. (4) The amount of dirty data of the RAID group (a) with smaller RG number is under "Dirty Data Stop Opportunity". And the amount of dirty data of the RAID group (b) which had a larger RG number than that of RAID group (a) is over "Dirty Data Stop Opportunity". (5) In the condition of (4), no random write commands are received in the RAID group (a) from a host and random write commands are received in the RAID group (b) from a host. "Dirty Data Stop Opportunity": [Storage Navigator Modular2]-[Performance]-[Tuning Parameter]-[System Tuning]-[Dirty Data Stop Opportunity] [Cause] Firmware bug. When the dirty data process checks the amount of dirty data sequentially from a RAID group with a smaller RG number to one with a larger RG number in order to write dirty data of each RAID group to HDDs, if the amount of dirty data in a RAID group is under "Dirty Data Stop Opportunity", the dirty data process does not write the dirty data in the RAID group to HDDs. However, due to the firmware bug, the first time the amount of dirty data in a RAID group is found under "Dirty Data Stop Opportunity", the dirty data process incorrectly stops checking the amount of dirty data in the remaining RAID groups and does not write any more dirty data to HDDs. As a result, when there are no available cache segments, host I/Os are not processed and then			

							<Countermeasure> Even when the amount of dirty data in the RAID group is found under "Dirty Data Stop Opportunity", the dirty data process continues to check the amount of dirty data in the remaining RAID groups to write dirty data in the RAID group to HDDs. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Follow the procedures below. (1) In case of not using Cache Partition Manager Set "Dirty Data Stop Opportunity" to 10% or under. Or turn PS OFF/ON. (2) In case of using Cache Partition Manager Turn PS OFF/ON. Or disable the Cache Partition Manager. (It is necessary to reboot the array to disable Cache Partition
	5	C	B	SD3362629	VA0-0176	The TC/TCE pair with copy speed "Fast" causes performance decreasing after copy is completed	[Phenomena] When managing TrueCopy(TC)/TrueCopy Extended Distance, the following phenomena may occur. (1) When copy TC/TCE pair with copy speed "Fast", Host I/O performance decreasing continues despite that pair status is changed to "Paired". <Equipment model / Firmware version> DF800/H, V4.0/A(0840/A) and later DF800EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Using TC/TCE (2) There are two or more P-VOLs (3) There are pairs that are controlled by same CTL but different core. (4) Create or Resync each pair mentioned in (3) with copy speed "fast" [Cause] Firmware bug. When copy speed is "fast", host I/O is limited for giving priority to copy. copy speed flag is used in each core for controlling host I/O limitation. There is firmware bug in logic of copy speed flag off when finishing copy. Judgment of finishing copy is executed in each CTL despite that it should be executed in each core. Then copy speed flag isn't changed to on in the core, which previously [Recovery] Apply the fixed firmware. <Action in the case of the failure> Execute one of the following operation (1) Reboot subsystem (2) Execute online firmware update (3) Execute one of the following operation, in each core of subsystem -Create pair, which has the P-VOL controlled by this core, with copy speed "middle" or "slow". -Resync the pair, which is controlled by this core, with copy
	6	C	B	-	VA0-0177	After PIN Over is recovered, DP Optimize may not be executed.	[Phenomena] After PIN Over is recovered, DP Optimize may not be executed. <Equipment model / Firmware version> DF800S/M/H V8.0/A(0880/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Dynamic Provisioning is enable (2) PIN Over is recovered (3) DP Optimize execute [Cause] Firmware bug. When DP Optimize execute, firmware refer to past PIN Over information. Therefore DP Optimize cannot execute even if PIN Over is recovered. <Countermeasure> Firmware correctly executes the execution judgment of the DP Optimize by current PIN Over information. [Recovery] Please apply the fixed firmware.

	7	C	C	-	VA0QA025	Though the model upgrade is not done, message "HH9V00 Model upgrade failed[Subsystem can not take over the user data.]" is issued when rebooting the array after the failure of initial setup.	[Phenomena] Though the model upgrade is not done, message "HH9V00 Model upgrade failed[Subsystem can not take over the user data.]" is issued when rebooting the array after the failure of initial setup. <Equipment model / Firmware version> DF700S/M/H, V1.1(V0711/A) and later DF800S/M/H/ES/EM/EH, All versions [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Wrong construction of the system disks (e.g. different type of disks or SED is included into the system disks.) (2) Initial Setup (3) The boot up of (2) is failed by (1) or other reasons (PS failure or so). (4) After (3), reboot the array without fixing the construction of the system disks. [Cause] Firmware bug. If initial setup is failed and the construction of the system disk is left illegal, the firmware can not detect the exact reason of the failure of rebooting and inadequate message is issued. <Countermeasure> When rebooting, if the construction of the system disk is illegal, [Recovery] Apply the fixed firmware. <Action in the case of the failure> If message "HH9V00 Model upgrade failed[Subsystem can not take over the user data.]" is issued though the model up is not done, check the construction of the system disk and fix to the right construction. Then execute initial setup or configuration clear.			
	8	C	B	EUC1270545	VA0-0183	A Head Diagnosis error may occur in a SAS HDD, and HDD blockade occurs.	[Phenomena] A Head Diagnosis error may occur in a SAS HDD, and HDD blockade occurs. I44100 The counter of intermittent HDU error was over the threshold(Unit-x,HDU-y)[DIAG] W09zab HDU alarm (Unit-x, HDU-y, Type-c) <HDD model / HDD Firmware version, Equipment model / Firmware version> HDD model / HDD Firmware version AKF400(S), 4C02 and later AKF400(S1), 4C01 and later AKH146(S)/AKH300(S), 4C56 and later AKH146(S1)/AKH300(S1)/AKH450(S), 4C54 and later AKH300(S2)/AKH450(S1)/AKH600(S)/AKH450X(S1)/AKH600X(S), 4C51 and later AWE2K(S)/AWE2KX(S), 5C04 and later Equipment model / Firmware version DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) SAS HDD [Cause] HDD firmware bug, Array firmware bug. When a Head Diagnosis process runs in an HDD, a Head Diagnosis error may occur by an intermittent HDD failure, and then an HDD blockade occurs because HDD firmware does not retry the Head Diagnosis process. An immediate HDD blockade may occur because array firmware does not execute Dynamic-sparing process before the HDD blockade. <Countermeasure> When a Head Diagnosis error occurs, HDD firmware retries Head Diagnosis process. When a value of Head Diagnosis errors exceeds the threshold, array firmware executes Dynamic-sparing process. [Recovery] Apply the fixed firmware.			
	V10.0/F, 08A0/F							2/18/2011	314	None
V10.0/F 08A0/F Base System V10.0/B, 08A0/B	1	I	-	-	-	The firmware strengthens the HDD recovery process for Head Diagnosis Error.	When Head diagnosis error (04/44F6 check condition response) is detected two times per day in an HDD I/O access, the firmware performs the dynamic sparing process.			
	V10.0/G, 08A0/G							3/10/2011	316	None

V10.0/G 08A0/G Base System V10.0/F, 08A0/F	1	C	A	SD3552529 SD3555477	VA0-0203	Data inconsistency issue due to dual HDD failure caused by LRC error.	[Phenomena] (a) HDD blockade due to LRC error Web message: IY0Hxy LRC error (Unit-x, HDU-y) or IY1600 LA/LRC error was detected(Unit-x, HDU-y) (b) Dual HDD failure due to LRC error Web message: IY0Hxy LRC error (Unit-x, HDU-y) or IY1600 LA/LRC error was detected(Unit-x, HDU-y) and I30100 HDU error (Unit-x, HDU-y) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) The firmware version is V9.0/A (0890/A) and later. (2) SATA HDD configured RAID1 or RAID1+0. The probability depends on a timing of write process for SATA HDD related to RAID1/1+0 configurations. Also when random write I/Os for near blocks are received [Cause] Firmware bug When write data has been written to master HDD configured RAID1 or RAID1+0 and it has not been written to mirror HDD yet, if new write data for near blocks is received, LRC code is created by using old data in the mirror HDD wrongly due to the firmware bug. When the invalid LRC code is written to only master HDD or only mirror HDD, the phenomenon (a) occurs. When the invalid LRC code is written to both HDDs, the phenomenon (b) occurs. If the phenomenon (b) occurs, after the one is blockaded, the media error (3/9001) is responded to a host when LRC error block is accessed. <Countermeasure> LRC code is created by using latest data. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Follow the procedures below. (1) Replace the failed HDD to a maintenance part. (Dummy replacement can be done, but it is difficult to isolate whether a cause of LRC error is the firmware bug or an actual HDD failure.) If correction copy succeeds, the recovery action completes. (2) If correction copy fails, please do the next action.			
	V10.0/J, 08A0/J							3/25/2011	317	None
V10.0/J 08A0/J Base System V10.0/G, 08A0/G	1	C	A	D800-28266 (SD3581137)	VA0-0206	Resync of TCE may not complete, then subsystem may go down due to "Kernel processing error" or "Watchdog timeout".	[Phenomena] (a) Resync of TrueCopy Extended Distance (TCE) may not complete. Host I/O can be run under the above situation. (b)Subsystem with S-VOL for TCE may go down due to "Kernel processing error" or "Watchdog timeout" after the phenomenon (a) occurred. Web message: HZ0N0x Kernel processing error(CTL-x) or H90320 Watch-dog time-out (c)And then status does not become "Ready" even if the array is rebooted repeatedly. <Equipment model / Firmware version> DF800S/M/H, V3.2/A (0832/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later			

							[Cause] Firmware bug (a)Resync of TCE does not complete. Subsystem with S-VOL for TCE has internal bifacial volumes in cache memory for a cycle data transfer, a creation and a deletion of their volumes are repeated each other. The deletion process may be running as a background job in Split status after pair split has been done. (The running of the deletion process cannot be confirmed by CE.) A notice of data transfer between P-VOL and S-VOL for TCE may not be done wrongly due to the firmware bug. The firmware bug may appear when Resync of TCE is done during the deletion process in case that Synchronizing status and Paired status are mixed in a CTG (Consistent Group). In the result, the data transfer process is repeated, however a Synchronizing pair cannot transit to Paired status, and Resync of TCE does not complete. (b)"Kernel processing error" or "Watchdog timeout" "Kernel processing error" or "Watchdog timeout" may occur, because a process that takes over one minute may be done in series wrongly when the data transfer process is repeated. The phenomenon may occur when the status that Resync of TCE does not complete is continued for a long time. A controller is blockaded due to "Kernel processing error" or "Watchdog timeout", then the same phenomenon occurs on the other controller, and			
	1	C	B	D800-54281	VB0-0377/VA0-0202	When the FC 8GB I/F port and FC-SW are connected, illegal number of BB_Credit is set to Switch.	[Phenomena] When the FC 8GB I/F port and FC-SW are connected, illegal number of BB_Credit is set to Switch. <Equipment model / Firmware version> DF800M/H, V7.2/A (0872/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] 1. FC 8Gbps I/F 2. FC-SW connection(PtoP topology) 3. Long-distance transmission with extender environment [Cause] Firmware bug The value that should be set with FC4Gbps I/F is set by mistake though the BB_Credit value is exchanged for Switch at FLOGI. <Countermeasure> A correct BB_Credit value is set at the Switch connection. [Recovery] Apply the fixed firmware. <Action in the case of the failure> None			
	V11.0/A, 08B0/A							4/8/2011	318	None
V11.0/A 08B0/A Base System V10.0/J 08A0/J	1	N	-	-	VB0-0011	2.5 inch expansion unit is supported.	2.5 inch expansion unit is supported.			
	2	N	-	-	VB0-0026	ShadowImage and SnapShot cascade configuration is supported.	ShadowImage and SnapShot cascade configuration is supported.			
	3	N	-	-	VB0-0091	TrueCopy pairsplit -RB option is supported.	TrueCopy pairsplit -RB option is supported.			
	4	I	-	SD3313575	VB0-0260	Deletion of LU mapped into H-LUN is prohibited. (Only at the time of LU deletion.)	LU mapped into H-LUN can not be deleted from HSNM2 in order to prevent unexpected access failure on hosts which use the LU.			
	5	I	-	-	VB0-0007	Improvement for the response time of the other I/F when command time-out occurs with plural interfaces configuration.	Improvement for the response time of the other I/F when command time-out occurs with plural interfaces configuration.			
	6	I	-	-	VB0-0389	When WriteSame commands are received at virtual LU, the guard function is disabled even if the specific WriteSame mode is OFF.	When WriteSame commands are received at virtual LU, the guard function is disabled even if the specific WriteSame mode is OFF.			
	7	I	-	DF800-27720 SD3412766	VB0-0381	Improvement for the ability of detecting failures of Enclosure.	Improvement for the ability of detecting failures of Enclosure.			
	8	I	-	-	VB0-0312	Non-volatility during power off and improvement of recovery process for inconsistency of HDP usage capacity with CTL blockade.	Non-volatility during power off and improvement of recovery process for inconsistency of HDP usage capacity with CTL blockade.			
	9	I	-	-	VB0-0127	WriteSame performance improvement (for RAID5 and RAID 6)	WriteSame performance improvement (for RAID5 and RAID 6)			
	10	I	-	-	VB0-0358	Error message is supported for Power Saving commands to RG consisted of SSDs.	Error message is supported for Power Saving commands to RG consisted of SSDs.			
	11	I	-	-	VB0-0268	Information for the average number of Tags and the maximum number of Tags is added to LU information of the performance statistical information.	Information for the average number of Tags and the maximum number of Tags is added to LU information of the performance statistical information.			
	12	I	-	-	VB0-0357	E-mail Alert model "AMSSMS" is renamed "StorageSystem".	E-mail Alert model "AMSSMS" is renamed "StorageSystem".			
	13	I	-	DF800-54295 EUC1260356	VB0-0327 V97-0320	Improvement for the precise indication of CPU utilization with adding the logic for correction of idle time when it was measured incorrectly.	Improvement for the precise indication of CPU utilization with adding the logic for correction of idle time when it was measured incorrectly.			
	14	I	-	DF800-28122 SD3532621	VB0-0009	Improvement for the value check of IP address on "equip_set" screen during the "Default setting" selection.	Improvement for the value check of IP address on "equip_set" screen during the "Default setting" selection.			
	15	I	-	-	VB0-0406	Improvement for the trace information of ShadowImage pairs. The firmware obtains its operational status and information on the tables for investigation if ShadowImage processes can not complete for a long time.	Improvement for the trace information of ShadowImage pairs. The firmware obtains its operational status and information on the tables for investigation if ShadowImage processes can not complete for a long time.			

	16	C	A	None	VB0-B011	Watchdog Timeout may occur when CTL is blockaded during host I/O with iSCSI I/F	[Phenomena] Watchdog Timeout may occur when CTL is blockaded during host I/O with iSCSI I/F. <Equipment model / Firmware version> DF800S/M/H, V1.0/A(0810/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) iSCSI I/F is equipped [Cause] Firmware bug When I/O process of Ready CTL conflicts with recovery process caused by CTL blockade, booting information to iSCSI I/F controller CHIP become incorrect and Ready CTL continues referring to invalid status, which results in the Ready CTL blockade and then system down. Countermeasure Timing of recovery process with CTL blockade is changed to prevent conflicts. [Recovery] Apply the fixed firmware. <Action in the case of the failure>
	17	C	A	None	VB0-0303	Data inconsistency with issuing write command(30MB+1KB or more) to PSUS(SP) pair of ShadowImage(SI).	[Phenomena] When write command in the length of 30MB+1KB or more is issued to PSUS(SP) pair of ShadowImage(SI), one of the following phenomena and dead lock may occur. Phenomenon A: Inconsistency of S-VOL Phenomenon B: Inconsistency of S-VOL+H90320 Watch-dog time-out Phenomenon C: Inconsistency of S-VOL+inconsistency of LU0 Phenomenon D: Inconsistency of S-VOL+HJ4ABS Microprogram error was detected[HDP] <Equipment model / Firmware version> DF800S/M/H/, V6.2/A (0862/A) or later DF800ES/EM/EH, V9.0/A (0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. [Common condition] - P-VOL or S-VOL whose pair status of SI is PSUS(SP) receives write command. - Write area of the above command is uncopied area or unformatted area.(Unformatted area is only for S-VOL.) - When write area of the above command is extended to the copy area of SI, the copy area is 32MB or more. [Individual condition] (1) Pair LU is normal LU. [Cause] Firmware bug When uncopied area of PSUS(SP) is written, area for HDP allocation, extent lock, quick format and PSUS copy is extended to the area of SI copy. If write command over 30MB is issued and extended to the area of SI copy, its length may be 32MB or more. Because the variable for the copy area is defined as USHORT, overflow may occur and the copy area may be reduced. As a result, HDP allocation, extent lock, quick format and PSUS copy is not executed with enough large area and the following phenomena may occur. Cause for each phenomenon Dead Lock: A conflict for segments with other jobs because the area of extent lock is not enough. Inconsistency of S-VOL: Write data is overwritten by back-ground quick format because the area of quick format issued by write job is not sufficient or the area where evacuation copy of S-VOL is not completed is overwritten because the area of PSUS(SP) copy is not sufficient. H90320 Watch-dog time-out: Unallocated area of HDP page is written because the allocated area of HDP page is not sufficient. Data Inconsistency of LU0(Normal LU): Unrelated LU0 is incorrectly written because the allocated area of HDP page is not sufficient. As a result, data inconsistency may occur if LU0 is normal LU. HJ4ABS Microprogram error was detected[HDP]: Unrelated LU0 is incorrectly written because the allocated area of

	18	C	A	None	VB0-0298	When S-VOL whose pair status of ShadowImage(SI) is PSUS(SP) receives write command, all pairs belonging to P-VOL is changed into PSUE status.	[Phenomena] In 1:N configuration of SI(i.e. Plural pairs belong to one P-VOL.), when S-VOL receives write command and HDP allocation to the S-VOL fails, not only S-VOL but all pairs belonging to P-VOL is changed into PSUE status. <Equipment model / Firmware version> DF800S/M/H/, V7.0/A (0870/A) or later DF800ES/EM/EH, V9.0/A (0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) SI 1:N configuration. (2) There is a pair in PSUS(SP) status. (3) P-VOL of the pair in PSUS(SP) status is virtual LU and its HDP pool is in temporary shortage ,which occurs during HDP pool format, or complete shortage. [Cause] Firmware bug If HDP page allocation to the S-VOL fails as write command to the S-VOL of a pair in PSUS(SP) status is received, only the S-VOL must be specified to be changed into PSUE status. Because P-VOL is specified for this, all pairs belonging to P-VOL is changed into PSUE status. Countermeasure Only S-VOL is specified for the status change. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform as follows. (1) Solve shortage of HDP pool for S-VOL changed into PSUE status.	
	19	C	A	D800-81733 SD3542802	VB0-0386	Pair operation of TrueCopy(TC) may fail after using clone function of VMware ESX.	[Phenomena] XCOPY command is issued at using clone function of VMware ESX. In case that data is copied to P-VOL of TC by the XCOPY command, operation of TC pair may result in failure with following message after the XCOPY command. [HSNM2 Message] DMER81003E: S-VOL command receiving. Wait a moment, then retry. [RAID Manager] Sense code: 9609 Detail code: x03E (x varies according to the pair operation.) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.3/A (0893/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) "UniqueExtendedCOPY" of host group option is enabled. (2) Original data and copied data of the XCOPY command belong to different CTL or core. [Cause] Firmware bug With write process at P-VOL of TC pair, the value of counter for management of duplication of write processes at S-VOL is added. Data copy of XCOPY must be executed with LUs belonging to the same core of the same controller. If the LU to which the data is copied belongs to the controller of the original LU, the counter must be reduced before it is added at execution of XCOPY command in order to operate LU exchange at first. This process of reduction is omitted, so that operation of TC pair is disabled because duplication of write processes at S-VOL is misjudged to be occurring. Countermeasure If LU exchange occurs at execution of XCOPY command, the counter is reduced. [Recovery] Apply the fixed firmware.	
	20	C	B	D800-28400 D800-81767	VB0-0407	It the subsystem down is generated by the Cisco connection.	[Phenomena] When the port of Cisco is out of order because of the connection, Cisco might put out the frame of the FC non-standard. MicroProgramError LSM is occured and the subsystem is downed. <Equipment model / Firmware version> DF800S/M/H V1.0/A(0810/A) or later DF800ES/EM/EH, V9.0/A (0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Fibre I/F (2) Switch is Cisco	

							[Cause] Firmware bug Because the place where LS_RJT should respond when the frame of the combination that the FC header that doesn't exist in the standard contradicts the payload is accepted is assumed to be illogicality of Firmware and you have blockaded the controller Countermeasure LS_RJT responds when the frame of the combination that the FC header contradicts the payload is accepted. [Recovery] Apply the fixed firmware. <Action in the case of the failure>		
	21	C	B	None	VB0-0352	The constant performance degradation of sequential read may occur with LU of SATA.	[Phenomena] The constant performance degradation of sequential read may occur, because multiplicity of staging is not allowed with SATA HDD. <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) or later DF800H, V4.0/A(0840/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) SATA HDDs are deployed (2) The ratio of dirty data within the RG having the LU is less		
							[Cause] Firmware bug Multiplicity of staged jobs must be 0 to boot the job staging function. With SATA HDD, maximum multiplicity of staged jobs per LU is 2 as default. However if one of the following conditions is fulfilled, the maximum multiplicity is 4. (1) The ratio of dirty data is less than 2%. (2) RG is expanding. When multiplicity of staged jobs is 4, maximum multiplicity of staged jobs misjudges it as error and initializes it to 0. Multiplicity of staged jobs is added at booting and reduced at ending, so that it becomes incorrect negative value when the execution is finished with 0 initialization. Once it becomes negative, it cannot return to 0 and the job staging function is disabled. This may cause the performance degradation of sequential read. Countermeasure With the process of reducing multiplicity of staged jobs, the multiplicity is modified to be 0 when it becomes negative. [Recovery] Apply the fixed firmware. <Action in the case of the failure>		
	22	C	B	None	VB0-0239	The performance degradation of copying may occur when the copy speed of SnapShot pair is "High".	[Phenomena] During SnapShot(SS) operation, copying of SS restore pair takes the same time as "Medium" copy speed although it is set to "High". <Equipment model / Firmware version> DF800H, V4.0/A(0840/A) or later DF800EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met.(Case 1) (1) During the SS operation. (2) There are two or more SS P-VOLs linked to different pools. (3) The SS P-VOLs at (2) belong to the same controller/core. (4) There is at least one pair with "High" copy speed among the SS P-VOLs at (2). (5) At least two P-VOLs among the SS P-VOLs at (2) is restored. (6) Host I/O is executed to the LU belonging to the same core of SS P-VOL under restoring. (7) One of the following conditions is fulfilled with a pair under restoring. - Shortage of DP pool or abnormal termination of the restore with error. - Cancelation of the restore for LU exchange performed by user. The problem may occur when all of the following conditions are met.(Case 2) (1) During the SS and TCE operations.		

							[Cause] Firmware bug Multiplicity of staged jobs must be 0 to boot the job staging function. With SATA HDD, maximum multiplicity of staged jobs per LU is 2 as default. However if one of the following conditions is fulfilled, the maximum multiplicity is 4. (1) The ratio of dirty data is less than 2%. (2) RG is expanding. When multiplicity of staged jobs is 4, maximum multiplicity of staged jobs misjudges it as error and initializes it to 0. Multiplicity of staged jobs is added at booting and reduced at ending, so that it becomes incorrect negative value when the execution is finished with 0 initialization. Once it becomes negative, it cannot return to 0 and the job staging function is disabled. This may cause the performance degradation of sequential read. Countermeasure With the process of reducing multiplicity of staged jobs, the multiplicity is modified to be 0 when it becomes negative. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Reset the power supply of the unit with performance degradation of
	23	C	B	DF800-54381 EUC1295516	VB0-0229	Controller blockades, caused by H-IPC hardware error, repeatedly occur.	[Phenomena] With H-IPC hardware error(iSCSI I/F error), controller0 or controller1 is blockaded repeatedly. <Equipment model / Firmware version> DF800S/M/H, V1.0/A(0810/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Equipped with iSCSI I/F. (2) Using LUN Manager. (3) Connecting the host unregistered to mapping ON/Target with [Cause] Firmware bug When discovery login from the unauthorized host fails at login authentication and the connection on/off is repeated, CHIP hardware reset occurs repeatedly because of CHIP firmware bug. This problem may occur when the threshold of CHIP hardware reset is exceeded. Countermeasure Firmware of iSCSI I/F controller will be modified. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Execute dummy replacement of the controller. Register iSCSI Name of connected host or do not connect
	24	C	B	None	VB0-0201	Watch-dog Timeout may occur when firmware is exchanged with host I/O.	[Phenomena] Watch-dog Timeout may occur when firmware is exchanged with host I/O. <Equipment model / Firmware version> DF800H, V4.0/A(0840/A) or later DF800EH,V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) DF800H/EH (2) IF#1 is equipped with iSCSI [Cause] Firmware bug One core may continue to refer to invalid data of another core when the processing times of the cores are different at firmware exchange because they are not synchronized. Countermeasure Synchronization between the cores are performed at firmware exchange. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Execute dummy replacement of the controller.

	25	C	B	None	VA0-0195 VB0-0360	"Good" is responded to incorrect Read Capacity command.	[Phenomena] When the parameter of Read Capacity command received from the host is incorrect, "Good " may be responded although "Check Condition" must be responded. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V3.0/A (0830/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) The host issues Read Capacity(6) or Read Capacity(10). (2) Above Read Capacity command has the following parameters. (2-1) PMI(Partial Medium Indicator) bit is ON. (2-2) The value of LBA is 0. Supplement) When PMI bit is ON, LBA must be Logical Block [Cause] Firmware bug LBA received from the host is not set to the table with Read Capacity commands. The value of LBA is checked if PMI bit is ON. Correct response is not sent because the unset table is referred. Countermeasure LBA received from the host is set to the table when Read Capacity(6) or Read Capacity(10) is received. [Recovery]
	26	C	B	None	VB0-S014	Controller blockade may occur when SnapShot(SS) pair is generated.	[Phenomena] Controller blockade may occur with following message when V-VOL is set to LUN of P-VOL and LUN of V-VOL of SS pair in Paired status is set to LUN of S-VOL in the operation of generating SS pair with auto-divided option. [Web Information Message] HJ2Cxy Microprogram error[POM] *xy is a number of the controller. <Equipment model / Firmware version> DF800S/M/H, V5.2/A(0852/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) P.P. of SS is unlocked. (2) RAID Manager or Hitachi Storage Navigator2 Command Line Interface is used as user interface. (3) LU(A) is set to P-VOL and LU(B) is set to S-VOL when SS pair(A) is generated. LU(A) is normal LU or virtual LU and LU(B) is V-VOL. (4) The status of SS pair(A) is "Paired" [Cause] Firmware bug Pool ID of P-VOL is checked at generation of SS pair. If LUN of V-VOL is set to the item for LUN of P-VOL, the check process for pool ID fails and controller blockade may occur. Countermeasure The check process for the status of LUN set to P-VOL is added before checking pool ID at generation of SS pair. [Recovery] Apply the fixed firmware. <Action in the case of the failure> (1) For RAID Manager: Check the configuration definition file. (2) For Hitachi Storage Navigator2 Command Line Interface:
	27	C	B	None	VB0-0347 VB0-0348	Maintenance port is not accessible or firmware exchange fails.	[Phenomena] Maintenance port is not accessible. If the problem occurs when firmware is exchanged with host I/O, the exchange may fail. <Equipment model / Firmware version> DF800S/M/H, V1.0/A(0810/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Access from HSNM2 or Web with maintenance port. (2) Firmware exchange with host I/O from HSNM2 with [Cause] Firmware bug At booting or rebooting the controller, it occasionally happen that maintenance port is not accessible because PHY of maintenance port is not reset. If it happens during firmware exchange with host I/O, the exchange may fail. Countermeasure Reset PHY of the maintenance port at booting the controller. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Detach LAN cable from the maintenance port and insert it again

	28	C	B	DF800-27862 DF800-27951 DF700-27893	VB0-0361	HSNM2 may become unavailable when HSNM2 and the array are connected with SSL communication.	[Phenomena] With firmware ver. 4.0/A or later, the following phenomena may occur. CLI: The execution of CLI command does not finish. GUI: The display does not change or it is not completed. <Equipment model / Firmware version> DF800S/M/H, V4.0/A(0840/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later, HSNM2 V4.00 or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Firmware ver. 4.0/A(0840/A) or later [Cause] Firmware bug In SSL process, HSNM2 waits for a response from the array without timer monitoring. If communication error or trouble in SSL process occurs, the operation of HSNM2 does not finish. There is the same problem with HSNM2. Countermeasure Timer monitoring function is added to both firmware and HSNM2, and time-out process is executed when no response is transferred. [Recovery] Apply the fixed firmware. <Action in the case of the failure> (a) Terminate HSNM2 as (a-1) or (a-2), then reboot it. (a-1) For HSNM2 GUI: Stop the service.(See HSNM2 User's guide.) (a-2) For HSNM2 CLI: Terminate the process forcibly with kill command or Ctrl+C. Then execute HSNM2 command again. (b) If the situation does not change with (a), wait 2 hours and retry (a). (c) If the situation does not change with (b), perform (c-1) or (c-2). (c-1) Replace the controller accessed by HSNM2 at dummy. (If the	
	29	C	C	None	VB0-B019	Hosts lost access after online microupdate with iSCSI I/F	[Phenomena] Hosts lost access after online microupdate with iSCSI I/F <Equipment model / Firmware version> DF800S/M/H V2.0/A(0820/A) or later DF800ES/EM/EH, V9.0/A (0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) iSCSI I/F (2)execute online microupdate (3)detect the hardware error of iSCSI protocol chip in online [Cause] Firmware bug When resetting the iSCSI protocol chips at the same time in online microupdate, the reset CTL number is incorrectly overwritten with other CTL number.As a result, it fails to firmware recovery , and hosts lost access. Countermeasure When resetting the dual iSCSI protocol chip at the same time,it start to reset the iSCSI protocol chip after completing the reset process of other I/F. [Recovery] Apply the fixed firmware. <Action in the case of the failure>	
	30	C	C	None	VB0-0409	iSCSI connection disconnected and reconnection was not acceptable on VMware.	[Phenomena] iSCSI connection disconnected and reconnection was not acceptable on VMware. Recconection had been available when virtual machine on Vmware rebooted. <Equipment model / Firmware version> DF800S/M/H V1.0/A(0810/A) or later DF800ES/EM/EH, V9.0/A (0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1)Using iSCSI protocol	

							[Cause] Firmware bug MaxCmdSN added to the iSCSI command was able to take the value of four bytes. It entered the state that the command is not generated because the handling when MaxCmdSN becomes a maxima violated the standard of iSCSI, and the connection cut. Countermeasure The method of updating the value when MaxCmdSN becomes a maxima is changed. [Recovery] Apply the fixed firmware. <Action in the case of the failure> (1)Execute explicit iSCSI Login.
	31	C	C	None	VB0-0411	After failure of enclosure occurs by backend diagnosis, performance may not recover even if the failure enclosure is replaced and recovered.	[Phenomena] The case enclosure failure occurs in process of backend diagnosis, enclosure that connected to "IN" port of failure enclosure keeps diagnostic state. After that, though the failure enclosure is replaced and recovered, array can not perform backend max performance because of enclosure that keeps diagnostic state. <Equipment model / Firmware version> DF800S/M/H V1.0/A(0810/A) or later DF800ES/EM/EH, V9.0/A (0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Hard errors occur in enclosure, and the enclosure failure occurs in process of backend diagnosis [Cause] Firmware bug The case enclosure failure occurs in process of backend diagnosis, firmware incorrectly keep the enclosure that connected to "IN" port of failure enclosure diagnostic state. Countermeasure When the backend diagnosis ends, firmware correctly clear diagnostic state. [Recovery] Apply the fixed firmware. <Action in the case of the failure> The case enclosure failure occurs with bellow Information Message, please dummy replace the enclosure connected to "IN" port of failure enclosure. Web message: I5H401 The search for the failure part of backend route error ended(Path-X,Route-Y) I5H000 Backend link error was detected(Unit-ZZ,ENC-Y) W0FA00 ENC alarm(Unit-ZZ,ENC-Y) :ENC /STR I5H301 The search for the failure part of backend route error
	32	C	C	None	VB0-0223	I/O may stop at firmware exchange with host I/O.	[Phenomena] I/O may stop at firmware exchange with host I/O. <Equipment model / Firmware version> DF800S/M/H, V2.0/A(0820/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Equipped with iSCSI I/F. (2) Firmware exchange with host I/O within 25 minutes after [Cause] Firmware bug When administration is moved from the rebooted controller to the "Ready" controller at firmware exchange with host I/O, there is a bug that the rebooted controller commands iSCSI I/F controller CHIP to transmit ARP. iSCSI I/F controller CHIP, referring the area of the "Ready" controller, detects incorrect report of completion. This incorrect completion causes the CHIP to be incapable of proceeding commands and I/O may stop. Countermeasure ARP transmission is restricted during firmware exchange with host I/O. [Recovery] Apply the fixed firmware. <Action in the case of the failure> I/O recovery operation is not necessary because it is performed after firmware exchange with host I/O.

	33	C	C	None	VB0-0284	Host Connector Alarm may occur.	[Phenomena] Host Connector Alarm for incorrect management information of equipment parts may occur. <web message> W0P702 Host connector alarm <Equipment model / Firmware version> DF800S/M/H, V1.0/A(0810/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when following (1) and one of (2)/(3) are met or (1) and (3) are met simultaneously. (1) Equipped with FC I/F. (2) Detachment, insertion or failure of following equipments. Power Unit/FAN/Battery/UPS/ENC/Expansion Unit (3) Replacement, insertion or failure of SFP. [Cause] Firmware bug There is no exclusion process for updating management information of equipment parts. After the controller update the data, other controller update it, so that inconsistency of the management information occurs. Countermeasure Exclusion logic is added with update of the management information. [Recovery] Apply the fixed firmware. <Action in the case of the failure>
	34	C	C	None	VB0-B015	Configuration copy is unable to be imported with unequipped configuration of IF#0.	[Phenomena] Configuration copy is unable to be imported with unequipped configuration of IF#0. <HSNM2 message> DMED1C0001: The process is disabled because iSCSI port is not equipped with. Check the port type and retry. <Equipment model / Firmware version> DF800S/M/H, V1.0/A(0810/A) or later DF800EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Other than DF800EM/ES. (2) IF#0 is equipped with iSCSI I/F. (3) Port0A is set for target#128. (4) Information collection (SCSI INQUIRY of IF#0 configuration) is executed. [Cause] Firmware bug Unnecessary check process for the target number is executed when change of mapping mode is requested at import of copy configuration, so that unequipped port set to target number of 128 or more is checked. Countermeasure Check function for the target number is disabled when change of mapping mode is requested. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Equip IF#0 with iSCSI I/F again, and delete the target of LUNM
	35	C	C	None	VB0-S014	Incorrect message may be displayed when SnapShot(SS) pair generation fails.	[Phenomena] For generation of SS pair, the operation fails if V-VOL is designated as both LUN of P-VOL and V-VOL. The message displayed with this failure is inappropriate. Followings are the incorrect messages. (1) SS pair generation: [HSNM2] DMER030068: Selected P-VOL has been paired with more than 1 V-VOL, specific POOL ID is different from allocated POOL ID. Check the POOL ID. [RAID Manager] Sense Code: 9608 Detailed Code: 0068 (2) SS pair generation with auto-divided option: [HSNM2] P-VOL, paired with more than 1 VOL, is commanded to generate a pair with the POOL ID different form allocated POOL ID. Check the POOL ID. [RAID Manager] Sense Code: 9608 Detailed Code: 007E <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) or later DF800H, V4.0/A(0840/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later

							[Cause] At SS pair generation, pool ID designated as P-VOL is confirmed by the check process. This confirmation may fail if LUN of V-VOL is set. And then, disk array sends inappropriate message code to HSNM2/RAID manager. Countermeasure The check process for LUN set to P-VOL is added before the confirmation process for pool ID. [Recovery] Apply the fixed firmware. <Action in the case of the failure> (1) For RAID Manager: Check the configuration definition file. (2) For Hitachi Storage Navigator2 Command Line Interface: Check the LUN of P-VOL.
	36	C	C	None	VB0-S014	Incorrect message may be displayed when TrueCopy Extended Distance(TCE) pair generation fails.	[Phenomena] At generation of TCE pair, if V-VOL is designated for LUN of P-VOL, the pair generation of TCE pair may fail. The message displayed with this failure is inappropriate. Followings are the incorrect messages. [HSNM2] DMER09008F: Specific POOL ID is different from allocated POOL ID. Check POOL ID. [RAID Manager] Sense Code: 9622 Detailed Code: 0020 <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) or later DF800H, V4.0/A(0840/A) or later DF800ES/EM/EH, V9.0/A(0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) P.P. of TCE and SnapShot is unlocked. (2) RAID Manager or Hitachi Storage Navigator2 Command Line
							[Cause] Firmware bug At TCE pair generation, pool ID designated as P-VOL is confirmed by the check process. This confirmation may fail if LUN of V-VOL is set. And then, disk array sends inappropriate message code to HSNM2/RAID manager. Countermeasure The check process for LUN set to P-VOL is added before the confirmation process for pool ID. [Recovery] Apply the fixed firmware. <Action in the case of the failure> (1) For RAID Manager: Check the configuration definition file. (2) For Hitachi Storage Navigator2 Command Line Interface:
	37	C	C	None	VB0-0191	ENC type and Device type are reported as "ENC type of Dense Unit" or "Device type of Dense Unit" by E-Mail when the array is booted with ENC blockade.	[Phenomena] E-Mail notification in which ENC type and Device type are described as "ENC type of Dense Unit" or "Device type of Dense Unit" is issued when the array is booted with ENC of RKAK blockaded. Unit type in the Message Code(W0Fze0) of Web message is also unspecified. <Equipment model / Firmware version> DF800S/M/H, V6.0/A (0860/A) or later DF800S/M/H/ES/EM/EH, V9.0/A (0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Using RKAK. (2) Rebooting the array. (3) Shut down without electricity.
							[Cause] Firmware bug When ENC blockade is detected at the early timing of booting process, the Unit type is not specified and regarded as Dense Unit. Countermeasure Firmware is modified to report correct Unit type. [Recovery] Apply the fixed firmware. <Action in the case of the failure> (1) Refer the Web message attached to the E-Mail. If the same part of ENC fails and the Unit type is not "Dense Unit", maintain according to that Web message. (2) Otherwise, maintenance staff brings all maintenance parts for the ENC of the array, check customer's failure ENC type and

	38	C	C	None	VB0-0276	Battery error detection is delayed when it is detached during auto-D/L of ENC firmware with single CTL.	[Phenomena] When battery is detached during auto-D/L of ENC firmware with single CTL, battery error is not detected until 10 minutes passed after the device status become READY. <Equipment model / Firmware version> DF800S/M/H V1.0/A(0810/A) or later DF800ES/EM/EH, V9.0/A (0890/A) or later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Single CTL configuration mode. (2) Other than DF800. (3) During auto-D/L of ENC firmware, the status of parts of Base [Cause] Firmware bug The hardware configuration changed flag is set at the timing of auto-D/L of ENC firmware starts. Battery error cannot be detected because the flag is incorrectly cleared with the check process of hardware configuration. Countermeasure Firmware is modified not to clear the hardware configuration changed flag. [Recovery] Apply the fixed firmware.			
	V10.0/M, 08A0/M							4/20/2011	326	None
V10.0/M 08A0/M Base System V10.0/J 08A0/J	1	I	-	-	-	LRC Error Check function support for the LU of SATA RAID1 and RAID1+0	This function is supported to prevent the potential of data inconsistency issue (ECN DF800-316) for the disk array system which has already been released with the firmware Ver.08A0/F and before. LRC Error Check function checks for the LU of SATA RAID1 and RAID1+0 whether there is LRC error block in (an) HDD(s). When LRC Error Check function has detected an LRC error block in (an) HDD(s), this function changes the block to a unreadable pinned (incomplete writing) data with the following WEB information message. W0L000 Unreadable PIN detected(Unit-xx,HDU-yy) I6L300 LRC error block was detected on the HDU(Unit-xx, HDU-yy) I6L301 at H-LUN-0001, Host LBA-0xaaaaaaaaaaaaaaaa, Drive LBA-0xbbbbbbbbbbbbbbbb or W0L000 Unreadable PIN detected(Unit-xx,HDU-yy) I6L500 LRC error block was detected on the HDU(Unit-xx, HDU-yy) and HDU(Unit-cc, HDU-dd) I6L501 at H-LUN-0001, Host LBA-0xaaaaaaaaaaaaaaaa, Drive LBA-0xbbbbbbbbbbbbbbbb The only members of Technical support center can perform the LRC Error Check function by the maintenance mode of Storage Navigator Modular 2 GUI Ver.10.07 and later (except Ver.11.00). LRC Check: Storage Navigator Modular 2 [Settings] - [LRC Check]			
	2	C	A	EUC1365100	VA0-0217	CTL blockade or array system outage caused by "Data pool wait time-out" or "Microprogram error[RVD]" may occur when DP-VOL of TCE/TC is used in VMware environment.	[Phenomena] (a) "HGA400 Data pool wait time-out" may occur and CTL may be blockaded. (b) Following (a), disk array system may go down. (c) "HJ2571 Microprogram error[RVD]" may occur at both controllers, then disk array system may go down. (d) After array system outage in (b)(c), the status does not become "Ready" even if the array is rebooted repeatedly. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.3/A (0893/A) and later [Conditions of Occurrence] (1) Conditions with TCE A. P-VOL of TCE is a DP-VOL B. The status of TCE is "PAIR". C. The P-VOL of TCE is used in VMware environment. (A Write Same command is received for P-VOL of TCE.) D. The configuration of TCE P-VOL is RAID 5or RAID6(except 2D, 4D, 8D or 16D). (The phenomena does not occur for RAID1 nor RAID1+0) E. The bandwidth of TCE path is set to 12Mbps or more. (2) Conditions with SS-TC(P-VOL of TC is V-VOL of SS.) A. P-VOL of SS is a DP-VOL B. The status of TC is "COPY". C. The P-VOL of TC is used in VMware environment. (A Write Same command is received for P-VOL of TC.) D. The configuration of SS P-VOL is RAID 5or RAID6(except			

							[Cause] Firmware bug Pool resources in a part of area for data transfer may not be released with TCE status of "PAIR" when P-VOL of TrueCopy Extended Distance(TCE), generated as Dynamic Provisioning (DP) volume, receives Write Same command issued by VMware operation in unallocated area of DP. Following this, CTL blockade or array system outage may occur with "Data pool wait time-out". Even if the array is rebooted, after this array system outage, the disk array system goes down before the status becomes "Ready" because the process continues and "Data pool wait time-out" occurs again. When the pool resources are not released, the disk array system may possibly go down because of "Microprogram error[RVD]". If P-VOL of TC is V-VOL of SS and P-VOL of SS is DP volume, "Data pool wait time-out" or "Microprogram error[RVD]" also may occur. The omission of releasing pool resources as above may occur when the boundary of stripes, described as follows, does not match the boundary of DP area depending on the timing (*1): For RAID 5 and RAID 6(except 2D, 4D, 8D or 16D), the boundary of DP area does not match the boundary of stripes because the boundary of stripes(as nD+1P, Stripe Size (64KB) xn) and the one of DP area(by 32MB) are different. (*2): The phenomenon may occur when the bandwidth of TCE/TC path is set to more than 12Mbps
	3	C	B	None	VA0-0237	PSUE may occur when TC copy is executed in a configuration of DP volume and 64KB stripe.	[Phenomena] PSUE of TrueCopy (TC) pair may occur when initial copy or resync of TC is executed. PSUE of TC pair may occur again when resync is executed after that PSUE. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.7/B (0897/B) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) TrueCopy configuration (TC P-VOL is not SS V-VOL.) A. TC P-VOL is DP volume in a DP pool with 64KB stripe (Default stripe size is 256KB.) B. The configuration of TC P-VOL is not 2D, 4D, 8D or 16D of RAID 5 or RAID6. (The problem does not occur with RAID1 and RAID1+0.) C. TC S-VOL is a Normal volume (not DP volume). D. TC pair is in initial copy or resynchronizing. E. There is unassigned area in DP volume for TC P-VOL (consumed capacity is less than the total capacity) (2) SnapShot-TrueCopy cascade configuration (TC P-VOL is SS V-VOL.) A. TC P-VOL is SS V-VOL. B. SS P-VOL is DP volume in a DP pool with 64KB stripe (Default stripe size is 256KB.) C. The configuration of SS P-VOL is not 2D, 4D, 8D or 16D of [Cause] Firmware bug When unassigned area for initial copy or resync of TrueCopy(TC) P-VOL, configured with Dynamic Provisioning(DP) volume and 64KB stripe, is transferred, the bit for differential data may not be cleared after this transfer. As a result, differential data is detected when all the bits for differential data are checked at completion of copy, then PSUE will occur. If TC P-VOL is configured with SS V-VOL and SS P-VOL is configured with DP volume, PSUE also may occur at TC copy. Above lack of the process of clearing the bit for differential data may occur at a stripe whose boundary does not match the boundary of DP area as follows. (*1): With other than 2D, 4D, 8D or 16D of RAID 5 or RAID 6, there may be a stripe whose boundary(=stripe size(64KB) xn [with nD+1P]) does not match the boundary of DP area(by 32MB). Countermeasure The process of clearing bits for differential data at transfer of DP volume unassigned area with TC was modified. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Operate the unit of TC P-VOL as follows. (1) Delete TC pair in PSUE.

	4	C	B	None	VA0-0213 (same as V11.0/A(08B0/A) VB0-0409)	iSCSI connection disconnected and reconnection was not acceptable on VMware.	[Phenomena] iSCSI connection disconnected and reconnection was not acceptable on VMware. Reconnection had been available when virtual machine on Vmware rebooted. <Equipment model / Firmware version> DF800S/M/H V3.2/E (0832/E) and later (except V11.0/A (08B0/A)) DF800ES/EM/EH, V9.0/A (0890/A) and later (except V11.0/A (08B0/A)) [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Using iSCSI protocol. [Cause] Firmware bug MaxCmdSN added to the iSCSI command was able to take the value of four bytes. It entered the state that the command is not generated because the handling when MaxCmdSN becomes a maxima violated the standard of iSCSI, and the connection closes. The host side stopped retrying because MaxCmdSN that the device added even if reconnected was not changed, and it became a reconnection not acceptable. Countermeasure The method of updating the value when MaxCmdSN becomes a maxima is changed. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Follow the procedures below. (1) Execute explicit iSCSI Login. (2) Reboot the host.			
	V11.0/B, 08B0/B							4/27/2011	334	None
V11.0/B 08B0/B Base System V11.0/A 08B0/A	1	I	-	-	VB0-0417	Improve the generation algorithm of TCP sequence number	TCP sequence number was generated by certain rule and there existed some possibility to predict the number. Now the number is generated randomly and the possibility is little.			
	2	I	-	D800-27865/54412 EUC1307328	VB0-0427	Improve the performance of SSL communication	Performance degradation might occur when communicating with Secure LAN Port on the firmware Ver. 9.0/A and later. Now the process of SSL communication is optimized. (Related Log:EUC1307328) The following shows SNM2 command response time with/without SSL. (A) Without SSL (a) Firmware All versions Less than 1sec (B) With SSL (a) Firmware(Ver 4.0/A) SSL certificate(*1) is Weak (Default) : Less than 3sec SSL certificate is Strong : Less than 26sec (b) Firmware(Ver 9.0/A) SSL certificate is Weak : Less than 3sec SSL certificate is Strong (Default) : Less than 26sec (c) Firmware(Ver 11.0/B) SSL certificate is Weak : Less than 3sec SSL certificate is Strong (Defaulut) : Less than 8sec *1 : Weak: RSA1024bit/SHA-1, Strong: RSA2048bit/SHA256 *2 : The result of displaying the list of LUs on a certain configuration. In general, command response time depends on the command and the configuration.			

	3	I	-	DF800-81734/81735 SD3552529 SD3555477	VB0-0431	LRC Error Check function support for the LU of SATA RAID1 and RAID1+0	This function is supported to prevent the potential of data inconsistency issue (ECN DF800-316) for the disk array system which has already been released with the firmware Ver.08A0/F and before. The firmware version 08A0/M, 08B0/B and later support this function. LRC Error Check function checks for the LU of SATA RAID1 and RAID1+0 whether there is LRC error block in (an) HDD(s). When LRC Error Check function has detected an LRC error block in (an) HDD(s), this function changes the block to a unreadable pinned (incomplete writing) data with the following WEB information message. W0L000 Unreadable PIN detected(Unit-xx,HDU-yy) I6L300 LRC error block was detected on the HDU(Unit-xx, HDU-yy) I6L301 at H-LUN-0001, Host LBA-0xaaaaaaaaaaaaaaaa, Drive LBA-0xbbbbbbbbbbbbbbbb or W0L000 Unreadable PIN detected(Unit-xx,HDU-yy) I6L500 LRC error block was detected on the HDU(Unit-xx, HDU-yy) and HDU(Unit-cc, HDU-dd) I6L501 at H-LUN-0001, Host LBA-0xaaaaaaaaaaaaaaaa, Drive LBA-0xbbbbbbbbbbbbbbbb The only members of Technical support center can perform the LRC Error Check function by the maintenance mode of Storage
	4	C	A	-	VB0-0430	HDD may be blockaded without appropriate recovery process when SAS HDD internal errors occur.	[Phenomena] HDD may be blockaded without appropriate recovery process when SAS HDD internal errors occur. <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. [Cause] Firmware bug When SAS HDD internal errors are detected and the value of the error threshold(10 times/day), which is managed by disk array, is exceeded, the drive is blockaded without executing dynamic sparing. Countermeasure The firmware was modified to execute dynamic sparing when it detects SAS HDD internal error for the 5 times in a day(2 times/day for SED HDD). [Recovery] Apply the fixed firmware. <Action in the case of the failure>
	5	C	A	None	VB0QA022	Data inconsistency issue due to a controller failure caused by LA error/DMA error/LRC error after an HDD media error	[Phenomena] When HDD media errors occur during HDD read process such as host I/O, the controller may be blockaded for LA error/DMA error/LRC error. After that, a check condition reply(4/4400) to host I/O may occur on another controller for LA error/DMA error/LRC error, then user data integrity may occur. When the controller is blockaded. H20100 Parity generation LA error[DRR] or HD5Exy Host transfer DMA error was detected(CTL-x,DMA-y) or HD27xy Drive Transfer DMA error over(DMA-XX When LA error/DMA error/LRC error occurs on another controller. W0N00x Parity generation LA error[DRR](CTL-x) or Wab0xy LRC error(H_PT-0x,CTL-y,TRNS-w) or Wab0xy LA error[errcode:LUN](H_PT-XX,CTL-Y,TRNS-X) or Wab0xy LA error[errcode:LBA](H_PT-XX,CTL-Y,TRNS-X) or Wab0xy LRC error(D_PT-XX,CTL-Y,TRNS-W) or Wab0xy LA error[errcode:LUN](D_PT-XX,CTL-Y,TRNS-W) or Wab0xy LA error[errcode:LBA](D_PT-XX,CTL-Y,TRNS-W) <Equipment model / Firmware version> F800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence]

							[Cause] Firmware bug When HDD media error is detected on the condition(2), all HDD read data is misjudged to be written to the cache because of the firmware bug. but read data which is not written to the cache is not deleted actually. So that, read data to be deleted may be incorrectly written to the cache when HDD read is executed with new host I/O etc. In this case, the controller may be blockaded for LA error/DMA error/LRC error when this incorrect data is used. On another controller, check condition reply(4/4400) to host I/O may occur for LA error/DMA error/LRC error in the same way, then User Data Integrity may occur. Countermeasure The firmware is modified to judge precisely whether all HDD read data is written to the cache when media error occurs, and to correctly discard unwritten read data if any. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Get backup data of the LU in which check condition reply(4/4400) occurs if necessary, then format it and restore the data.
	6	C	A	None	VB0-0416	System outage or data inconsistency may occur when errors occur during the process of RG expansion.	[Phenomena] When controller blockade or interruption of power occur during RG expansion, system outage or data inconsistency may occur. <Equipment model / Firmware version> DF800S/M/H, V5.2/A (0852/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later DF800S/M/H/ES/EM/EH, V11.0/B (08B0/B) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. System outage may occur on the following conditions. (1) Controller blockade or interruption of power occur during RG expansion. (2) There is no LU with the same number of the RG under expansion process in the array. Data inconsistency may occur on the following conditions. (1) Controller blockade or interruption of power occur during RG expansion. [Cause] Firmware bug RG expansion process updates the information of LUs before it remaps the data of LUs in the RAID group. When controller blockade or interruption of power occur during the process of updating the information, error recovery process of RG expansion is executed. However , the first LBA of unexpanded area is set to an incorrect value because there is a bug of the computing logic for the recovery process. Accordingly, if an LU with the same number of the RG under expansion process is created in the array, data inconsistency may occur because the LBA of unexpanded area is mistaken. If there is no LU with the same number of the RG under expansion process in the array, controller blockade may occur because of exception of division by zero, then the system may goes down. Countermeasure The computing logic for the LBA of the recovery process, which is executed when errors occur during the update of LUs information, will be modified. [Recovery] Apply the fixed firmware. <Action in the case of the failure>

	7	C	A	DF800-54535/28446 EUC1365100	VB0-0420	CTL blockade or array system outage caused by "Data pool wait time-out" or "Microprogram error[RVD]" may occur when DP-VOL of TCE/TC is used in VMware environment.	[Phenomena] (a) "HGA400 Data pool wait time-out" may occur and CTL may be blockaded. (b) Following (a), disk array system may go down. (c) "HJ2571 Microprogram error[RVD]" may occur at both controllers, then disk array system may go down. (d) After array system outage in (b)(c), the status does not become "Ready" even if the array is rebooted repeatedly. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.3/A (0893/A) and later [Conditions of Occurrence] This problem may occur when all of the following conditions are met. (1) Conditions with TCE A. P-VOL of TCE is a DP-VOL B. The status of TCE is "PAIR". C. The P-VOL of TCE is used in VMware environment. (A Write Same command is received for P-VOL of TCE.) D. The configuration of TCE P-VOL is RAID 5or RAID6(except 2D, 4D, 8D or 16D). (The phenomena does not occur for RAID1 nor RAID1+0) E. The bandwidth of TCE path is set to 12Mbps or more. (2) Conditions with SS-TC(P-VOL of TC is V-VOL of SS.) A. P-VOL of SS is a DP-VOL B. The status of TC is "COPY". C. The P-VOL of TC is used in VMware environment. [Cause] Firmware bug Pool resources in a part of area for data transfer may not be released with TCE status of "PAIR" when P-VOL of TrueCopy Extended Distance(TCE), generated as Dynamic Provisioning (DP) volume, receives Write Same command issued by VMware operation in unallocated area of DP. Following this, CTL blockade or array system outage may occur with "Data pool wait time-out". Even if the array is rebooted, after this array system outage, the disk array system goes down before the status becomes "Ready" because the process continues and "Data pool wait time-out" occurs again. When the pool resources are not released, the disk array system may possibly go down because of "Microprogram error[RVD]". If P-VOL of TC is V-VOL of SS and P-VOL of SS is DP volume, "Data pool wait time-out" or "Microprogram error[RVD]" also may occur. The omission of releasing pool resources as above may occur when the boundary of stripes, described as follows, does not match the boundary of DP area depending on the timing (*1): For RAID 5 and RAID 6(except 2D, 4D, 8D or 16D), the boundary of DP area does not match the boundary of stripes because the boundary of stripes(as nD+1P, Stripe Size (64KB) xn) and the one of DP area(by 32MB) are different. (*2): The phenomenon may occur when the bandwidth of TCE/TC	
	8	C	B	None	VB0-0421	PSUE may occur when TC copy is executed in a configuration of DP volume and 64KB stripe.	[Phenomena] PSUE of TrueCopy (TC) pair may occur when initial copy or resync of TC is executed. PSUE of TC pair may occur again when resync is executed after that PSUE. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.7/B (0897/B) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) TrueCopy configuration (TC P-VOL is not SS V-VOL.) A. TC P-VOL is DP volume in a DP pool with 64KB stripe (Default stripe size is 256KB.) B. The configuration of TC P-VOL is not 2D, 4D, 8D or 16D of RAID 5 or RAID6. (The problem does not occur with RAID1 and RAID1+0.) C. TC S-VOL is a Normal volume (not DP volume). D. TC pair is in initial copy or resynchronizing. E. There is unassigned area in DP volume for TC P-VOL (consumed capacity is less than the total capacity) (2) SnapShot-TrueCopy cascade configuration (TC P-VOL is SS V-VOL.) A. TC P-VOL is SS V-VOL. B. SS P-VOL is DP volume in a DP pool with 64KB stripe (Default stripe size is 256KB.) C. The configuration of SS P-VOL is not 2D, 4D, 8D or 16D of	

							[Cause] Firmware bug When unassigned area for initial copy or resync of TrueCopy(TC) P-VOL, configured with Dynamic Provisioning(DP) volume and 64KB stripe, is transferred, the bit for differential data may not be cleared after this transfer. As a result, differential data is detected when all the bits for differential data are checked at completion of copy, then PSUE will occur. If TC P-VOL is configured with SS V-VOL and SS P-VOL is configured with DP volume, PSUE also may occur at TC copy. Above lack of the process of clearing the bit for differential data may occur at a stripe whose boundary does not match the boundary of DP area as follows. (*1): With other than 2D, 4D, 8D or 16D of RAID 5 or RAID 6, there may be a stripe whose boundary(=stripe size(64KB) xn [with nD+1P]) does not match the boundary of DP area(by 32MB). Countermeasure The process of clearing bits for differential data at transfer of DP volume unassigned area with TC was modified. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Operate the unit of TC P-VOL as follows. (1) Delete TC pair in PSUE. (2) Apply the modified firmware.			
	9	C	B	None	VB0QA056	When ENC Firmware of 2.5 inch expansion unit is exchanged, the ENC may be blockaded.	[Phenomena] When ENC Firmware of 2.5 inch expansion unit is exchanged, the ENC may be blockaded. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.0/A(08B0/A) and later [Conditions of Occurrence] The problem may occur when one of the following conditions is met. (1) The firmware, whose ENC Firmware is updated, of 2.5 inch expansion unit is exchanged with host I/O. (2) The firmware, whose ENC Firmware is updated, of 2.5 inch expansion unit is exchanged in maintenance mode, then the array [Cause] ENC Firmware bug There is a bug that the process of rebooting the ENC takes incorrectly much time after the ENC Firmware was exchanged. Because of this, ENC blockade may occur if the process of rebooting the ENC does not finish within the time-out period. Countermeasure The reboot process of ENC Firmware is modified to finish the process of booting within the time-out period. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Replace the blockaded ENC.			
	10	C	C	None	VB0-0418	Incorrect countermeasure against the vulnerability of SSL algorithm.	[Phenomena] Even if the firmware V9.0/A or later, which is modified for the Year 2010 problem of encryption, is used, LAN ports of DF can be accessed by using vulnerable algorithm DES_CBC_SHA. Some security scanners detect usage of this algorithm as vulnerability. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are [Cause] Firmware bug The Year 2010 problem for Web ports is not handled. Countermeasure DES_CBC_SHA is deleted in the algorithm used by Web ports. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Apply the fixed firmware.			
	V11.3/A, 08B3/A							5/20/2011	340	None
V11.3/A 08B3/A Base System V11.0/B 08B0/B	1	N	-	-	None	DKSA2; 10Gbps iSCSI I/F Board support	10Gbps iSCSI I/F is supported. (Except for DF800S, M)			
	2	I	-	SD3552529 SD3555477	VB3-0006	Improvement of HDD data recovery function in case that an HDD blockade occurs before/during LRC Error Check	In an old (V10.0/M and V11.0/B) firmware, HDD data recovery (correction copy) process fails, when an HDD blockade occurs before/during LRC Error Check and an LRC error block is detected during the recovery process with HDD replacement. In new firmware, the recovery process can be proceeding and partially completed because an LRC error block is changed to Unreadable PIN block in the replaced HDD. Please refer to a document "DF800 LRC Error Check Tool Recovery Procedure Rev.1" for the detailed operating procedures of LRC Error Check function.			

	3	I	-	EUC1365100	VB3-0012	Add recovery logic of CTL blockade or disk array system outage caused by "Data pool wait time-out" or "Microprogram error[RVD]"	This function is supported to recover CTL blockade or disk array system outage issue for the disk array system which has already been released with the firmware Ver.08A0/F and before. The firmware version 08B0/B and later support this function. When this issue is occured, wrong management data is left at the disk array system. Therefore the same phenomenon occurs again even if reboot the disk array system. After support this function, change pair status of SS/TC/TCE to PSUE and refer following message in substitution for CTL blockade . I6L800 Invalid Data pool information was detected(LU-XXXX) XXXX: LU Number Please refer to Early Notice DF800-EN-M062.
	4	I	-	SD3581137	VB3-0013	Add recovery logic of disk array system outage issue	This function is supported to recover disk array system outage issue due to "Kernel processing error" or "Watchdog timeout" for the disk array system which has already been released with the firmware Ver.08A0/G and before. The firmware version 08A0/J and later support this function. When this issue is recovered by applying this firmware, the pair of TCE becomes PSUS with Read/Write restricted (Inconsistent), and the pair of SnapShot becomes PSUE(Failure) and notices the following WEB information message. I6L700 The invalid management information of Snapshot function was detected Please refer to Early Notice DF800-EN-M061.
	5	I	-	-	VB3-0019	The operation of "Crossing operation CPU load decrease mode" is made Default. .	In the firmware version upgrade to this version or later, operation by Default becomes regardless of "Crossing operation CPU load decrease mode". Please refer to DF800-EN-M046 for details
	6	I	-	-	VB3-0020	Add the process to clear diagnostic state if an enclosure is kept diagnostic state incorrectly. (related log: V11.0/A VB0-0411)	The case enclosure failure occurs in process of backend diagnosis, firmware incorrectly keeps the enclosure that connected to "IN" port of failure enclosure diagnostic state. (related log: V11.0/A VB0-0411) In V11.0/A firmware, when the backend diagnosis ends, firmware correctly clears diagnostic state. In this improvement, firmware clears diagnostic state about
	7	C	A	None	VB3-0011	In a synchronization of a TrueCopy pair including virtual LU, uncopied areas remain after the Pair transition.	[Phenomena] In a synchronization of a TrueCopy pair including virtual LU, uncopied areas remain in the S-VOL after the pair transition when both Hitachi Dynamic Provisioning and TrueCopy are used. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.3/A (0893/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) One of the following conditions is met. (a) P-VOL of TC is virtual LU. (b) P-VOL of SS in a cascade configuration where V-VOL of SnapShot(SS) is set as P-VOL of TC is virtual LU. (c) S-VOL of TC is virtual LU. (d) P-VOL of SS in a cascade configuration where V-VOL of SnapShot(SS) is set as S-VOL of TC is virtual LU. (2) One of the followings is met. (a) Creation/re-synchronization is executed to the TC pair of (1)-(a) or (1)-(b). (b) SWAP re-synchronization is executed to the TC pair of (1)-(c) or (1)-(d). [Cause] Firmware bug At the data transfer, the progress status is managed by using the progress bitmap for each specific capacity. When Write Same command is accepted, virtual LU area is released even during the data of the synchronization is forwarded. At this time, even if the data transfer of this released area is not finished, the transfer is interrupted and the transfer of next area is started. In this case, the data already transferred in the previous area is incorrectly judged as completed because the same progress bitmap is used. <Countermeasure> The process in the case of Write Same command is accepted in an area where data transfer is not completed is modified as follows: The area is released after the data transfer was completed, then the copy of next area starts. [Recovery] Apply the fixed firmware. <Action in the case of the failure>

	8	C	A	None	VB3-0010	Data inconsistency may occur when XCOPY command is issued to the ShadowImage(SI) pair in PSUS(SP) status.	[Phenomena] When XCOPY command is issued to the S-VOL of SI pair in PSUS(SP) status and the S-VOL is set as a source of the XCOPY, the source data and the copy data of the XCOPY are inconsistent. (The copy data of the XCOPY is incorrect.) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.3/A (0893/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) SI is enabled. (2) The RAID group of the SI pair is RAID1 or RAID1+0, and the stripe size is not 64KB. (3) The SI pair is in PSUS(SP) status. (4) XCOPY command is issued by VMware operation. (5) XCOPY command is issued to the S-VOL of SI pair at (2), [Cause] Firmware bug If the copy range of the XCOPY includes uncopied area of the PSUS(SP) pair, the XCOPY copies incorrect area. <Countermeasure> When the uncopied area is included, the process of correcting the copy area is added. [Recovery] Apply the fixed firmware or disable the special Extended Copy mode.
	9	C	A	None	VB3-0007	When XCOPY is issued to a resident LU, CTL blockade or performance degradation of the resident LU may occur.	[Phenomena] When XCOPY command is issued to a resident LU of Cache Residency Manager(CRM), the following phenomena may occur. Phenomenon A: CTL blockade Web message: HF0700 Data transfer check error[LU OWNERSHIP] Phenomenon B: The controller of the resident LU is changed and the LU become not resident, then its performance is degraded. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. Phenomenon A (1) The destination LU of XCOPY command is a resident LU. Phenomenon B (1) CRM is enabled. (2) XCOPY command is issued by VMware operation. [Cause] Firmware bug Phenomenon A The XCOPY command refers incorrect data because it obtained segments in an incorrect way. Data transfer check error occurs as a result. Phenomenon B Even though the controller of a resident LU must not be changed, LU for XCOPY is not checked if it is resident. The controller of a resident LU is changed as a result. <Countermeasure> Phenomenon A XCOPY to the resident LU is responded with Check condition. Phenomenon B The change of the controller of the resident LU is responded with Check Condition, so that XCOPY is prevented from changing the controller of the resident LU. [Recovery] Apply the fixed firmware or disable the special Extended Copy mode. <Action in the case of the failure> Phenomenon A (1) Stop issuing the XCOPY command. (2) Replace the blockaded controller with new one. Phenomenon B

	10	C	A	None	VB3QA001	When unified LU accepts a WriteSame command issued by VMware operation, CTL may be blockaded with Microprogram error[RAD].	[Phenomena] When the LU having sub logical unit such as unified LU accepts a WriteSame command issued by VMware operation, CTL may be blockaded with Microprogram error[RAD]. If the WriteSame command is retried, another CTL is blockaded and the subsystem goes down. Web message: HJ120M Microprogram error[RAD] <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.0/A (08B0/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) The special WriteSame mode of the host group option or the iSCSI Target option is enabled. (2) A WriteSame command issued by VMware operation is accepted for the end of the LU. (3) The LU accepting the command has sub logical unit. (4) The LU accepting the command is not P-VOL nor S-VOL of ShadowImage pair, SnapShot pair, TrueCopy pair, TrueCopy Extended Distance pair or Modular Volume Migration pair. Note to (3): The way to create the LU having sub logical unit. (a) Increase the capacity of LU. (b) Unify plural LUs. [Cause] Firmware bug WriteSame commands save target area in the memory. WriteSame commands separate the target area and execute the process for each separated area, then update the target area in the memory when each process is completed. In this process, the area to be updated is distinguished with the address and the length of the completed area. In the case of the LU having sub logical unit, the address must be converted. With this bug, however, when a WriteSame command executes the process for the end of the LU having sub logical unit, it refers to incorrect address at the timing of address conversion of the sub logical unit. Therefore, the CTL is blockaded. <Countermeasure> The firmware is modified not to execute the process of updating the target area but to delete the target data itself when WriteSame commands completed the process of all target area. [Recovery] Apply the fixed firmware. <Action in the case of the failure>	
	11	C	B	None	VB3-0023	When "Command Unique Response Mode" is Enable, the controller blockage is generated by the IO operation.	[Phenomena] When "Command Unique Response Mode" is Enable, the controller blockage is generated by the IO operation. HJ080B Microprogram error[FSM] HH7Dxy Microprogram error[ISM] <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) "Command Unique Response Mode" is Enable (2)The unexecution command that has passed 1.5 seconds since the command was [Cause] Firmware bug The unexecuted command that accepts the command when the special response mode is effective and passes 1.5 seconds responds in Check Condition, and management information on the host command is purged. The command responds from the other queue of management information on the host command when read command fails by the drive input-output time-out. As a result, because the command that has already responded is executed, and the controller is blockaded. <Countermeasure> When check condition responds, the queue is previously purged from the other queue of management information. [Recovery] Apply the fixed firmware. <Action in the case of the failure>	

	12	C	B	None	VB0QA061	When a TrueCopy Extended Distance(TCE) pair is created, resynchronized or swapped, virtual LU utilization of S-VOL may become incorrectly high.	[Phenomena] When TCE pair whose P-VOL and S-VOL are virtual LU is created, resynchronized or swapped, virtual LU utilization of S-VOL at the timing of copy completion may become incorrectly high in comparison with that of P-VOL. In addition, it may take more time to complete the copy process in comparison with the pair whose P-VOL and S-VOL are normal LU. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.3/A (0893/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Both P-VOL and S-VOL of the TCE are virtual LU. (2) P-VOL of the TCE belongs to the DP pool of RAID5 or RAID6. (3) P-VOL of the TCE belongs to the DP pool whose data disks are not 2D, 4D, 8D or 16D. [Cause] Firmware bug TCE process sequentially transfers data from the beginning by 256KB. The data transfer area of the TCE pair can span the page boundary or the end of chunks. The data beyond the boundary or the end of chunk is zero data and not necessary to be transferred, but the boundary and the end is not correctly detected because of this bug, then the zero data is transferred incorrectly. As a result, the virtual LU utilization of S-VOL become higher than that of P-VOL. Because the transfer is not correctly managed during the area, which is beyond the page boundary or the end of chunk, is transferred, area already transferred may be transferred again. Therefore it takes more time to complete the copy process. <Countermeasure> The firmware is modified to correctly detect the page boundary and the end of chunk in order not to operate incorrect transfer. [Recovery] Apply the fixed firmware. <Action in the case of the failure> For the S-VOL whose virtual LU utilization is incorrectly high			
	13	C	B	EUC1352266	VB3-0005	Degradation of I/O performance may occur because certain registers of ASIC of CTL fail.	[Phenomena] Degradation of I/O performance may occur because certain registers of ASIC of CTL fail. <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are [Cause] Firmware bug Because of the failure of the registers, the light is not emitted with host I/O. In this case, Link initialization, executed by the host, inevitably fails. Every time the host repeatedly executes Link initialization, Link initialization at host I/F port is also executed, therefore CPU utilization rises. As a result, degradation of I/O performance occurs. <Countermeasure> The firmware is modified to detect the failure of registers and not to execute Link initialization repeatedly. [Recovery] Apply the fixed firmware.			
	V11.5/A, 08B5/A							6/24/2011	349	None
V11.5/A 08B5/A Base System V11.3/A 08B3/A	1	N	-	-	VB5-0001	3TB SATA HDD is supported.	3TB SATA HDD is supported.			
	2	I	-	EUC1363350	VB5-0097	Tuning Parameter enhancement	"Load Reduction for Changing Configuration Mode" is supported as a new System Tuning of Tuning Parameter. This mode is disabled by default. When this mode is enabled, the effects for host I/O performance caused by SNM2 (or SNM2 API) operations are reduced and SNM2 operations are subject to restrictions. See also 8. Notes. (1-a) Operations for changing configurations may be processed once in 30 seconds when the load of array's CPU is more than or equal to 10%. A user may not receive the information from the array because SNM2 operation is slow down. If multiple SNM2 accesses to an array, such slowing down on an SNM2 will affect to other SNM2. (1-b) Slowing down the pace to delete DP-volume processing in the background; - Usually 1TB DP-vol deletion will take 5 seconds. - With this mode is enabled, 1TB DP-vol deletion will take about 200 seconds. Until the end of the deletion, DP-vol which has the same LUN of deleting DP-vol can not be created.			
	3	I	-	-	VB5-0086	Countermeasure for the system rebooting after the system goes down during RG expansion.	If an error occurs because of controller blockade or power failure during the process of RG expansion, both systems may go down. The countermeasure of ECN334#3 was applied for this. If system goes down before applying modified firmware, the system can be rebooted with installation of the modified firmware			

	4	I	-	SD3508105 SD3548582	VB5-0022	Host recognition during I/O is supported.	The function for automatic recognition of host connected with FC during I/O is supported. See Hardware user's guide "7.12 Platform-Specific Parameter Settings". "Disable Autodiscover New HG Mode" is supported in Port
	5	I	-	SD3763875	VB5-0102	Improvement of the message for capacity shortage at DP-VOL creation/expansion.	The message has been changed as follows when the DP-VOL creation/expansion of system is beyond the maximum capacity. Before improvement: DMED0E0021: The capacity of specified area is insufficient. Please confirm the capacity and then try again. After improvement: DMED0E002C: The process cannot be performed because the specified capacity will exceed the capacity of the subsystem. Please specify the capacity within the range of
	6	I	-	-	VB5-0002	Controllability of HDP pool is adapted for acceleration.	The system response time was improved when executing DP pool creation, addition, deletion, and re-initialization. Before improvement: The system response time depends on the DP pool capacity. After improvement: The system response time doesn't depend on
	7	I	-	-	VB5-0075	Specification of the response for pool exhaustion is changed.	After the DP pool is completely depleted, accessible condition is met as follows. Before improvement: The free capacity of DP pool becomes 5% or more of the total capacity. After improvement: When DP pool capacity is more than 2TB, free capacity will be 100GB.When DP pool capacity is fewer than
	8	I	-	-	VB5-0017	LU exchange management of XCOPY command is changed.	It may take times to spin up the drive when XCOPY command, issued by VMware operation, exchanges LU. The LU exchange process of XCOPY command is modified to improve the time for spinning up the drive.
	9	I	-	-	VB5QA006	Improvement of response time and error messages of SNM2 commands when controller 0 is rebooting	Before improvement: Protocol sequence error (DMEA000004) or time-out error (DMEA000007) is displayed in SNM2 in case of time-out error of a SNM2 command. After improvement: The response time of a SNM2 command during controller 0 rebooting is improved and the possibility of time-out error is reduced. If the connection error (DMEA000006) is displayed in SNM2 in case of time-out error, a command retry is
	10	C	A	SD3745803	VB5-0080	Link Up cannot be performed after the firmware exchange with I/O.	[Phenomena] Link Up cannot be performed after firmware exchange with host I/O and then host access lost may occur. In this case, initialization process of Link is incorrectly repeated and CPU utilization rises so that problems such as I/O degradation of ports not troubled occur. <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H,V4.0/A(0840/A)and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) 4G FC-I/F is used. (2) The transmission speed of DF is fixed.(4G, 2G or 1G)(default: Auto) (3) The firmware is exchanged with host I/O. [Cause] Firmware bug When firmware is exchanged with host I/O, the transmission speed is incorrectly set to the initialized value (1GBps) in recovery process after Chip Reset, caused by itermittent hardware errors, is executed with Fibre I/F. As a result, inconsistency between the transmission speed and that of the host may occur. In this case, because Link Up is disabled, initializing of Link is repeatedly executed and the CPU utilization rises. <Countermeasure> Set the transmission speed to the original correct settings but not the information initialized at the firmware exchange with host I/O. [Recovery] Apply the fixed firmware. <Action in the case of the failure>
	11	C	A	EUC1404652	VB5-0085	When Cache Partition Manager is used with DF800H/EH, if there are three or more partitions whose segment sizes are the same, host access error or controller failure may occur.	[Phenomena] When Cache Partition Manager is used with DF800H/EH, if there are three or more partitions whose segment sizes are the same, [1]host access error or [2]controller failure may occur. Web message [1] Host access error: None [2] Controller failure: Microprogram error[RCH] <Equipment model / Firmware version> DF800H, V4.0/A (0840/A) and later DF800EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) DF800H/EH (2) Cache Partition Manager is enabled. (3) There are three or more partitions whose segment sizes are the same and at least one of them belongs to each controller. (4) LU in the partitions receives a write command. [2] The following condition is necessary only for controller failure. (5) Firmware exchange with host I/O, firmware exchange during

							[Cause] Firmware bug If LU is changed when there is dirty data of write process in the cache, pair partitions of both controllers lend cache segments to the other temporarily. In case of host I/O utilization is high, the borrowed cache segments are not returned to the original pair partition and may be reused for other LU in the same partition. [1] Host access error If the borrowed cache segment is reused for other LU and the cache segment is lent for LU change, it may return not to the original partition but to other partition in the same DIR. In this case, if firmware exchange with host I/O, firmware exchange during processing with rebooting, controller failure, ENC failure, CHK1 or PS OFF without cache volatilization occurs, DIR is changed. However, the number of the segments for host I/O is incorrectly set to 0 because there is a bug of count logic for number of available segments in this DIR. As a result, Host I/O fails. [2] Controller failure In the case of there are multiple borrowed cache segments in a partition and each segment originally belongs to different partition, when the cache segments are returned at a same time, if the returned cache segments except first one conflict segment transfer from other CPU core, cue error of the segment occurs because there is a bug of exclusive control logic for resources in the partition where the segments are returned to. As a result, the controller fails. <Countermeasure>
	12	C	A	None	VB5-0020	When the system drive is SSD or SAS7.2K, the array may not be booted.	[Phenomena] When the system drive is SSD or SAS7.2K, even though there is no mix of different types of drives, the array may not be booted. Web message HH9Q00 The system drives are composed of different types of drives <Equipment model / Firmware version> DF800S/M/H, V8.0/A (0880/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) The system drive is SSD or SAS7.2K. (2) At the timing of booting the array, at least one drive of system drives fails and at least one drive is normally completed when [Cause] Firmware bug SSD and SAS7.2K are recognized as SAS drives before Inquiry command for distinguishing drive types is issued. If the inquiry command fails, they continue to be recognized as SAS drives. As a result, the array cannot be booted because intermixture of SAS drives is incorrectly detected at the intermixture check. <Countermeasure> System drives blockaded for Inquiry command are not checked by intermixture check because their drive types are not distinguished. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Replace or perform dummy replacement of the failed system drives and then reboot the array. For the failed drives, please refer to "Disk Drive" of "Parts Information" in the WEB(http:// IP address of the array). The
	13	C	A	None	VB5QA015	The array cannot be booted after PS off.	[Phenomena] The array cannot be booted after PS off. <Equipment model / Firmware version> DF800S/M/H, V6.5/A (0865/A) and later DF800ES/EM/EH,V9.0/A(0890/A)and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) DM-LU is created, DP pool is created or there is a large amount of PIN data. (2) The array is booted with one of the (1) conditions [Cause] Firmware bug There is a bug that Linkdown of drives cannot be detected between drive spin up and Ready status of the array. After the drive spin up, DM-LU read, HDP pool information read and drive access for staging PIN data is executed, but the drives are not blockaded if they are in Linkdown. In this case, the commands to the drives continues and process of the array booting does not progress. <Countermeasure> If Link errors occurs with drives at the timing of booting the array, the drives are blockaded. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Enter maintenance mode and install the fixed firmware then boot

	14	C	A	None	VB5QA008	Both controllers failures occur with Microprogram error[RCH] during Write commands for LU of RAID5 or RAID6 configured with SATA HDDs is executed, and the array system down may occur.	[Phenomena] The following phenomenon may occur with the firmware V6.0/A (0860/A) or later. Controller failure may occur during Write commands for LU of RAID5 or RAID6 configured with SATA HDDs. After that, the other controller failure also occurs and the array system may go down. In the case of the array system down occurs, even if the array is rebooted with its cache unvolatilized, both controllers failures occur again and then the array system down may occurs. In this case, the cache has to be volatilized for recovery of the array. As a result, data inconsistency issue may occur. HJ11xx Microprogram error[RCH] <Equipment model / Firmware version> DF800S/M/H, V6.0/A (0860/A) and later DF800S/M/H/ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) The firmware version is V6.0/A (0860/A) and later. (2) SATA HDD (3) RAID5 or RAID6 (Except DP pool for Dynamic Provisioning) (4) Capacity of one LU configured with one RAID group exceeds the following capacity and Write commands are received in the field over the capacity. (4-1) LU over 64TB with 16KB cache segment [Cause] Firmware bug In order to process dirty data of successive host LBAs collectively, HDD write process searches for cache segment of dirty data whose host LBA is next to the dirty data. In this process, the search is performed with 4 byte address because of the bug while 8 byte is appropriate, so that the incorrect cache segment of 4 byte address is reserved. As a result, an error is detected in reserved segment check at parity creation, and then controller failure may occur with Microprogram error[RCH]. After that, if the same process is executed on the other controller before the dirty data of the 4 byte address cache segment is written to HDD, controller failure may occur and the array system goes down. In the case of the array system down occurs, even if rebooting of the array is tried, the array cannot be rebooted because the same action is processed. <Countermeasure> In HDD write process, dirty data is correctly searched for with the 8 byte address cache segment. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Before release of the fixed firmware (1) If the controller failure occurs, perform dummy replace of the controller.
	15	C	B	None	VB5-0112	CUDG error may occur at the timing of booting the array implemented with 10G iSCSI I/F.	[Phenomena] When the array implemented with 10G iSCSI I/F is booted, CUDG error occurs with the below message and the controller is blockaded. Web message HA0100 CUDG error(CTL-x) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.3/A(08B3/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) 10G iSCSI I/F is implemented. (2) PS/ON of the array is performed [Cause] Firmware bug If read process of FirmwareBootloader from DDR3 memory fails at initializing of the protocol chip, initializing of the protocol chip fails because the read process is not retried. <Countermeasure> If read process of FirmwareBootloader from DDR3 memory fails, the process is retried. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform dummy replacement of the controller.

	16	C	B	None	VB5-0110	If P-VOL receives XCOPY command or ATS command during COPY process of virtual LU ShadowImage(SI) pair or Modular Volume Migration(MVM) pair, controller blockade may occur.	[Phenomena] If P-VOL receives XCOPY command or ATS command during initial copy, resynchronization or restoration of virtual LU SI pair or initial copy of virtual LU MVM pair, controller blockade may occur with the following message. Web message HJ4AXX Microprogram error was detected[HDP](CTL-X) or HJ11XX Microprogram error[RCH] <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.3/A (0893/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) SI or MVM P.P. is enabled. (2) Dynamic Provisioning(DP) is enabled. (3) A pair of SI or MVM is created. (4) A copy target LU of the pair is virtual LU. (5) The pair is in following conditions. (a) SI pair: Initial copy, resynchronization or restoration is being processed.(i.e. The pair status is Synchronizing, Paired Internally Synchronizing or Reverse Synchronizing.) (b) MVM pair: Copy is being processed.(i.e. The pair status is Copy.) (6) XCOPY command(as a target) or ATS command is issued to the P-VOL of the pair by using VMware. (7) There is a DP unallocated field in a copy target LU of the pair. [Cause] Firmware bug This problem occurs because background copy, which is copy process executed in background to achieve consistency of original data and copied data in initial copy or resynchronization of SI or MVM, exceeds the process fields of XCOPY command or ATS command. If fields where background copy is not completed receives XCOPY command or ATS command, XCOPY command or ATS command hands over the copy process at the copy target to the background copy. However, if XCOPY command or ATS command is overtaken by background process, it exchanges the process and execute data copy to the copy target. At that time, if the target LU is a virtual LU and unallocated, allocation of physical fields is not performed. As a result, a logical error occurs at the data copy process and then the controller is blockaded. <Countermeasure> XCOPY command or ATS command performs allocation process of physical fields regardless of the progress of the background copy if the copy target is an unallocated field. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Refer to [redacted] of the controller manual.
	17	C	B	None	VB5-0110	If P-VOL receives ATS command during COPY process of virtual LU ShadowImage(SI) pair or Modular Volume Migration(MVM) pair, controller blockade may occur.	[Phenomena] If P-VOL receives ATS command during initial copy, resynchronization or restoration of virtual LU SI pair or initial copy of virtual LU MVM pair, controller blockade may occur with the following message. Web message HJ4AXX Microprogram error was detected[HDP](CTL-X) or HJ11XX Microprogram error[RCH] <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.3/A (0893/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) SI or MVM P.P. is enabled. (2) Dynamic Provisioning(DP) is enabled. (3) A pair of SI or MVM is created. (4) A copy target LU of the pair is virtual LU. (5) The pair is in following conditions. (a) SI pair: Initial copy, resynchronization or restoration is being processed.(i.e. The pair status is Synchronizing, Paired Internally Synchronizing or Reverse Synchronizing.) (b) MVM pair: Copy is being processed.(i.e. The pair status is Copy.) (6) ATS command is issued to the P-VOL of the pair by using VMware. (7) There is a DP unallocated field in a copy target LU of the pair.

							[Cause] Firmware bug This problem is caused by incorrect judgment of necessity for physical field allocation. When ATS command is issued to fields where background copy, which is which is copy process executed in background to achieve consistency of original data and copied data in initial copy or resynchronization of SI or MVM, is completed, physical fields are allocated and then data copy process is performed if the target LU is a virtual LU and unallocated. However, if the fields where background copy is completed and the fields where the ATS command is issued match, allocation of physical fields is not performed because of incorrect judgment . As a result, a logical error occurs at the data copy process and then the controller is blockaded. <Countermeasure> ATS command performs allocation process of physical fields regardless of the progress of the background copy if the copy target is an unallocated field. [Recovery] Apply the fixed firmware. <Action in the case of the failure>
	18	C	B	SD3511253	VB5-0100	When ENC or controller is exchanged, the message of cable error is displayed incorrectly, so that it may take times for maintenance.	[Phenomena] If LinkDown occurs with ENC not exchanged when other ENC or controller is exchanged, the message of cable error is displayed incorrectly, so that it takes times for maintenance. <Web message> HH9N01 ENC recovery failed[Cable error](CTL-X) or I5HB00 ENC recovery failed[Cable error](Unit-YY, ENC-Z) X: Controller number, YY: Unit number, Z: ENC number <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH,V9.0/A(0890/A)and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1)At least one expansion unit is connected. (2) ENC or controller is exchanged. (3) LinkDown occurs with ENC other than exchanged one. (4) The following messages are displayed and exchange of ENC or controller fails. <Web message> HH9N01 ENC recovery failed[Cable error](CTL-X) [Cause] Firmware bug A process that determines the configuration of connection is executed during a controller recovery process. If LinkDown occurs in this process, the web massage of cable error is incorrectly displayed. <Countermeasure> The firmware is modified not to display the web message of cable error for LinkDown detected by ENC at determining the configuration of connection. Additionally, the following messages are displayed in case of ENC LinkDown. Web message At controller insertion: HH9Y01 ENC recovery failed[linkup error in the other route](CTL-X) At ENC insertion: I5JJ00 ENC recovery failed[linkup error in the other route](Unit-YY,ENC-ZZ) X: Controller number YY: Unit number ZZ: ENC number [Recovery] Apply the fixed firmware. <Action in the case of the failure> (1) Check the cable connection of the controller or ENC described in the Web message. Web message HH9N01 ENC recovery failed[Cable error](CTL-X)
	19	C	B	None	VB0QA059	LinkDown may occur with the ENC because it takes times for booting process of the ENC Firmware, so that the ENC is blockaded.	[Phenomena] LinkDown may occur with the ENC because it takes times for booting process of the ENC Firmware, so that the ENC is blockaded. Web message I5HC00 ENC error was detected[Linkdown](Unit-XX,ENC-Y) W0FE30 ENC alarm(Unit-XX,ENC-Y)W01400 CTL alarm(CTL-X) X: Unit number, Y: ENC number <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.0/A (08B0/A) and later [Conditions of Occurrence] The problem may occur when one of the following conditions are met. (1) Firmware of 2.5 inch expansion unit whose ENC Firmware is updated is exchanged with I/O.

							[Cause] ENC Firmware bug There is a bug that it takes many times to boot ENC Firmware at booting ENC of 2.5 inch expansion unit. Because of this, ENC may not be booted in the time limit of timeout and ENC is blockaded for LinkDown. <Countermeasure> The rebooting process of ENC Firmware is modified to complete its booting in the limit of timeout. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Replace the blockaded ENC.
	20	C	B	None	VB5-0095	The controller is blockaded during optimization of DP pool.	[Phenomena] The controller may be blockaded during optimization of DP pool. Web message HJ4Axx Microprogram Error was detected[HDP] (xx: code, y:CTL#(0-1)) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Dynamic Provisioning is enabled. (2) DP pool optimization for virtual LU is performed. (3) Write Same command or Unmap command to virtual LU is received or SnapShot pair is deleted when virtual LU of (2) is used as SnapShot pool. [Cause] Firmware bug The format of original pages for DP pool optimization should be performed by the core of virtual LU but there are cases that it is performed by other core. <Countermeasure> The format of original pages for DP pool optimization is certainly performed by the core of virtual LU. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Cancel the DP pool optimization and perform dummy replacement of the blockaded controller then apply the fixed firmware. After
	21	C	B	None	VB5-0082	Host Connector Alarm may occur when the array implemented with 10G iSCSI I/F is booted.	[Phenomena] Host Connector Alarm may occur when the array implemented with 10G iSCSI I/F is booted. Web message Host connector alarm (Port XY) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.3/A(08B3/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) 10G iSCSI I/F is implemented. (2) PS/ON of the array is performed. (3) Notice of Host Connector implementation is received during a [Cause] Firmware bug After booting of a command for protocol chip is completed at initial setup, internal management information of Host Connector is changed to the status for receiving Host Connector notification. However, if the command is received before completion of the command, the notification is incorrectly ignored because the status has not been changed to the status for receiving Host Connector notification. As a result, Host Connector Alarm occurs. <Countermeasure> SFP implementation asynchronous event is not received before completion of the command not to be ignored. [Recovery] Apply the fixed firmware. <Action in the case of the failure>

	22	C	B	None	VB5-0109	If P-VOL receives write command during resynchronization of ShadowImage(SI) pair, the SI pair may be changed to PSUE incorrectly.	[Phenomena] If P-VOL receives write command during resynchronization or restoration of SI pair, the SI pair is incorrectly changed to PSUE with the following message at completion of the resynchronization or the restoration. Web message IG0000 PSUE occurred(LU-XXXX/YYYY) <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) SI is enabled. (2) Resynchronization(including Quick Resynchronization) or restoration of SI pair is being executed. (3) Write access to the P-VOL of SI pair. (4) One of the following conditions is met. (a) Failure(controller failure, CHK1 or PS OFF without volatilization) occurs. (b) S-VOL is a normal LU and Quick Format is performed for it. (c) Both P-VOL and S-VOL are normal LUs. P-VOL is not [Cause] Firmware bug In synchronization and restoration process, a pointer indicating the area where differential data copy is completed is updated after a pointer indicating LBA executing differential data copy is updated. In case of P-VOL receives write access between the two updates, there might be some data not copied to S-VOL. When differential data copy of whole area is completed, a pointer indicating the area where differential data copy is completed is updated. If P-VOL receives write access during this process, there might be some data not copied to S-VOL in the same way. In this case, the SI pair change to PSUE because this inconsistency is detected by data consistency check at completion of pair transition. <Countermeasure> The pointer indicating the area where differential data copy is completed is updated first to prevent data not being copied to S-VOL. [Recovery] Apply the fixed firmware. <Action in the case of the failure>
	23	C	C	None	VB5-0074	When Host Connector Alarm occurs, alarm LED <Red> of Host Connector incorrectly goes out.	[Phenomena] When Host Connector Alarm occurs with Host Connector error or disconnection of it, Alarm LED <Red> of Host Connector is turned on but it incorrectly goes out after a while. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.3/A(08B3/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) 10G iSCSI I/F is implemented. (2) Host Connector Alarm occurs. (3) Shutdown process of iSCSI Firmware triggered by (2) is not [Cause] Firmware bug When Host Connector error or disconnection is detected, Alarm LED should be turned on and iSCSI Firmware should be terminated. If this termination of iSCSI Firmware is not completed, it is forcibly terminated by resetting a protocol chip but the Alarm LED is incorrectly turned off in this reset process. <Countermeasure> When the reset process is executed with Host Connector error or disconnection, Alarm LED is turned on again after the reset. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform maintenance procedures as Web message. Web message:
	24	C	C	None	VB5-0093	The Alarm message for excess of virtual threshold may not be displayed while using AccelerateWideStripingMode.	[Phenomena] There is a case that the Alarm message of virtualization excess threshold may not be displayed while using AccelerateWideStripingMode, so that exhaustion of capacity for virtual LU creation cannot be detected beforehand. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V10.0/A (08A0/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Dynamic Provisioning is enabled. (2) WideStripingMode is enabled.

							[Cause] Firmware bug Consumption of DP pool capacity with WideStripingMode may become larger than that of virtual LU so that virtualization excess threshold should be calculated with consideration of that, but there is a bug that the value is underestimated. As a result, the following Web messages may not be displayed. Web Message I6GK00 Over Provisioning Ratio Forewarning (Pool-XX) I6GL00 Over Provisioning Ratio Overwarning (Pool-XX) XX: Pool number <Countermeasure> For LU where WideStripingMode is enabled, virtualization excess threshold is calculated by rounding up by 1GB for each DP-RG. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Set the value of virtualization excess threshold higher or increase			
	V11.5/B, 08B5/B							7/17/2011	358	None
V11.5/B 08B5/B Base System V11.5/A 08B5/A	1	I	-	SD3670376	VB5-0076	It added HDU blockade condition by media error at Lower Drive Detach Threshold Mode.	HDU blockade condition by media error detection at Lower Drive Detach Threshold Mode. Before improvement : Verify threshold over. After improvement: Verify threshold over and Command timeout threshold over to HDU			
	2	C	A	SD3720808	VB5-0101	The host may detect the command reply error by host I/O performance degradation during dynamic sparing.	[Phenomena] The host may detect the command reply error by host I/O performance degradation of drive reply delay during dynamic sparing. <Equipment model / Firmware version> DF800S/M V3.2/E (0832/E) and later DF800H V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Execution of dynamic sparing . (2) A lot of media errors are detected by the read of the drive by dynamic sparing. [Cause] Firmware bug When drive media error is detected by recover processing of dynamic sparing, firmware does not update reassign count because of design gives priority to data recovery. Even though a lot of media errors found by recover processing of dynamic sparing, HDD blockade cannot be made by error when threshold exceeds the certain value. For this reason, collection resonse cannot be changed if other drives are used in raid group. <Countermeasure> When drive media error is detected by recover rocessing of dynamic sparing, firmware update reassign the count because the design gives priority to host I/O response. HDD blockade can be made by error when threshold exceeds the certain value. It becomes possible to change collection response used in other drives in raid group. [Recovery] Apply the fixed firmware. <Action in the case of the failure>			
	3	C	A	SD3670376	VB5-0083	There is a probability of decreasing host I/O performance if many media error occur on successive LBAs in a HDD.	[Phenomena] There is a probability of decreasing host I/O performance if many media error occur on successive LBAs in a HDD. <Equipment model / Firmware version> DF800S/M V3.2/E (0832/E) and later DF800H V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) SATA HDD			

							[Cause] Firmware bug Current firmware counts reassign count for threshold value with starting dynamic sparing of HDD. Regarding SATA HDD, firmware doesn't manage media error occurrence correctly because firmware counts one count with 64 blocks as a unit if there are multi media error in a "64 blocks". So firmware counts media error smaller than real media errors counts incorrectly. <Countermeasure> Firmware counts up by the number of reassigning blocks for starting dynamic sparing threshold. (Not detected media error counts because of avoiding the repetition of counting the same media error block) [Recovery] Apply the fixed firmware. <Action in the case of the failure> [Before V9.7/C(0897/C)] None [V9.7/C(0897/C) and later] Please enable Lower Drive Detach Threshold Mode for being
	4	C	A	None	VB5-0124	A Controller is blockaded wrongly when booting up the controller.	[Phenomena] An error of hardware diagnosis is detected on a controller wrongly and the controller is blockaded when booting up the controller. <Web message> HA010x CUDG error(CTL-x) CACHE#0 ECC data line error[OWN_CTL] DCTL hard error[OWN_CTL][DCTL] or another message. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.5/A (08B5/A) [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) When booting up a controller as PS ON of an array or installing the controller. The probability of the occurrence of this [Cause] Firmware bug During a cache diagnosis of a controller, another cache access caused by a LAN processing will interrupt and conflict with the cache diagnosis. As results, a diagnosis error is detected wrongly. <Countermeasure> The condition of the LAN interruption is fixed. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Execute the dummy replace of the blockaded controller or the
	5	C	B	SD3717120	VB5-0113	When it executes online firmware update, controller may be blockaded with Microprogram error[FTD].	[Phenomena] When it executes online firmware update, controller may be blockaded with Microprogram error[FTD]. <Web message> HJ0707 Microprogram error[FTD] <Equipment model / Firmware version> DF800S/M V3.2/E (0832/E) and later DF800H V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1)FC-I/F (2) Controller blockaded is occurred in resetting the protocol chip [Cause] Firmware bug When controller blockaded is occurred while resetting the protocol chip, there is the bug that doesn't clear reset state . As a result, the firmware falsely detect the inconsistency while checking the state at online firmware update. <Countermeasure> The firmware initialize the reset state in rebooting a system. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Execute the offline firmware update after dummy replace the

	6	C	B	SD3828016	VB5-0116	When data transfer timer is expired , controller may be blockaded with Microprogram error[HSC].	[Phenomena] When data transfer timeout is occurred , controller may be blockaded with Microprogram error[HSC]. <Web message> HJ0AFD Microprogram error[HSC] <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.0/A (08B0/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1)Data transfer timer except for Read/Write command is expired (timeout value is (3(s))). (2)The timer for Aborting to the protocol chip is expired(timeout [Cause] Firmware bug In spite of the firmware have to respond the status ,but the firmware falsely detect the inconsistency and blockaded controller. <Countermeasure> The firmware respond the status in condition of occurrence. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy replace the blockaded controller.
	7	C	B	None	VB5-0108	XCOPY commands may not be executed to the LU for which the access restriction is changed by using Data Retention Utility(DRU).	[Phenomena] XCOPY commands issued to the LU for which the access restriction is changed by using DRU may incorrectly be responded with Check Condition. Otherwise, the sense key or the sense code of the Check Condition in response may be incorrect. In the case that Check Condition in response is incorrectly returned, the sense key/sense code is one of the followings. (05/2200), (07/2700) In the case of incorrect Check Condition in response, the sense key/sense code is (05/2200).The sense key/sense code which should be returned is originally (07/2700). <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Host group option or UniqueExtended COPY option of iSCSI Target option is enabled. (2) An XCOPY command is issued by using VMware. When above (1) (2) and below (3) is met, the XCOPY command is incorrectly responded with Check Condition. (3) The source LU or the target LU of the XCOPY command meet the one of the following conditions. (a) The source LU of the XCOPY command is set to S-VOL Disable mode. [Cause] Firmware bug XCOPY commands are not executed when Check Condition is returned according to Read Inhibition attribute of DRU for the source LU of XCOPY commands and Write Inhibition attribute of DRU for the target LU of XCOPY commands. However, Check Condition returned even when an attribute other than Read Inhibition attribute or Write Inhibition attribute is given. As a result, XCOPY commands are incorrectly responded with Check Condition or incorrect sense key/sense code is returned. <Countermeasure> The process of response for Check Condition is modified to be returned according to Read Inhibition attribute for the source LU of XCOPY commands and Write Inhibition attribute for the target LU of the XCOPY commands. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Disable UniqueExtendedCOPY option of Host Group option or
	8	C	B	None	HDS-109	In case sequential I/O is run for the two or more LUs which are in one and the same RAID Group and whose owner cores are different, the command response delay may occur in the DF800H/EH.	[Phenomena] In case sequential I/O is run for the two or more LUs which are in one and the same RAID Group and whose owner cores are different, the command response delay may occur in DF800H/EH. <Equipment model / Firmware version> DF800H/EH, V9.3/A(0893/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Firmware version is V9.3/A(0893/A) and later. (2) The model are DF800H and DF800EH. (3) The LUs coreX owns and those that coreY owns do not exist in one and the same RAID Group.

							[Cause] Firmware bug The owner core requests the issue of command to a drive. In case of the drive in the chassis which coreX owns, firmware checks for the request of comand issue from coreX that the command can be issued, but it does not checks for that from coreY wrongly. The number of commands which can be issued at a time is described below. - SAS HDD, SAS7.2K HDD, SSD, SED are 30. - SATA HDD is 6. Highly-loaded sequential I/O is run for some LUs at the same time, the response of drive can easily be delayed and drive queue depth is remained in full. As a result, there is possibility that a command from the core which does not check is forced to have a long wait. <Countermeasure> Firmware checks for the request of comand issue from both coreX and coreY that the command can be issued. [Recovery] Apply the fixed firmware. <Action in the case of the failure> The ownership of LUs are changed in order that the LUs coreY
	9	C	B	None	VB5-0119	The performance degradation may be occurred when Link failure occurs repetitively.	[Phenomena] The performance degradation may be occurred when Link failure occurs repetitively. <Equipment model / Firmware version> DF800S/M V3.2/E (0832/E) and later DF800H V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1)FC-I/F [Cause] Firmware bug When Link failure is occured,the firmware issue the Link initialize in cycles of 100(ms). In this sequence, it may take about 100(ms) to control the LED of FC interface board. As a result,it raise the CPU-hogging and the performance degradation may be happened. <Countermeasure> The firmware doen't control the LED of FC interface board in this condition of occurrence. [Recovery] Apply the fixed firmware. <Action in the case of the failure>
	10	C	B	None	VB5-B001	When it excutes online firmware update, controller may be blockaded with Microprogram error[ISD].	[Phenomena] When it excutes online firmware update, controller may be blockaded with Microprogram error[ISD]. <Web message> HH7F06 Microprogram error[ISD] <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.3/A (08B3/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1)10G iSCSI-I/F (2)Online firmware update is exucted (3)iSCSI protocol chip detect the error in initilizing the iSCSI [Cause] Firmware bug When iSCSI protocol chip detect the error in initilizing the iSCSI firmware, in spite of it's possible to retry the initialization, the firmware doen't retry the iSCSI firmware initialization. <Countermeasure> Retry the iSCSI firmware initialization. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy replace the blockaded controller.

	11	C	B	None	VB5-0117	Head Diagnosis error occurs in the SAS HDD, and then HDD blockade may occur.	[Phenomena] Head Diagnosis error occurs in the SAS HDD, and then HDD blockade may occur. <Web message> HDU error report(Unit-X,HDU-Y)[04-44F2] HDU intermittent error over(Unit-X,HDU-Y) <Equipment model / Firmware version> For HDD firmware AKH146(S)/AKH300(S), 4C61 and later AKH146(S1)/AKH300(S1)/AKH450(S), 4C5C and later AKH300(S2)/AKH450(S1)/AKH600(S)/AKH450X(S1)/AKH600X(S), 5C57 and later [Conditions of Occurrence] The problem may occur when all of the following condisions are met. (1) SAS HDD (2)Head Diagnosis conflicts in HDD when receiving multiple Read/Write commands at the same time. Head Diagnosis error [Cause] HDD Firmware bug. Due to the defect, other Head Diagnosis may be executed while Head Diagnosis in the process. Head Diagnosis error (04/44F2) occurs because Head Diagnosis process leads to the unexpected result. <Countermeasure> Modification will be made for the Head Diagnosis in order not to execute other Head Diagnosis incorrectly while processing. [Recovery] Apply the fixed firmware. <Action in the case of the failure>			
	12	C	C	None	VB5-0096	Parameter "Dirty Data Flush Number Limit" can not be changed to "Disable".	[Phenomena] Parameter "Dirty Data Flush Number Limit" can not be changed to "Disable", even if "Initialize Parameters" function is executed when the parameter is set to "Enable". <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.7/A (0897/A) and later [Conditions of Occurrence] The problem occurs certainly when all of the following conditions are met. (1) Firmware version V9.7/A (0897/A) and later (2) Parameter "Dirty Data Flush Number Limit" is set to "Enable". (default setting: Disable) Storage Navigator Modular 2-[Performance]-[Tuning Parameter]-[System Tuning]-[Dirty Data Flush Number Limit] (3) "Initialize Parameters" function is executed with Storage Navigator Modular 2. Storage Navigator Modular2-[Performance]-[Tuning [Cause] Firmware bug "Initialize Parameters" process does not initialize the setting value of parameter "Dirty Data Flush Number Limit". <Countermeasure> "Initialize Parameters" process initializes the setting value of parameter "Dirty Data Flush Number Limit" to set the parameter to "Disable". [Recovery] Apply the fixed firmware. <Action in the case of the failure> Execute "Edit System Turning Parameters" function to set parameter "Dirty Data Flush Number Limit" to "Disable".			
	V11.5/D, 08B5/D							8/28/2011	366	025
V11.5/D 08B5/D Base System V11.5/B 08B5/B	1	I	-	None	VB6-0002	Default value is changed about the Port Option "Disable Autodiscover New HG mode".	-Before V11.5/D: The default value of this mode is "OFF". -V11.5/D and later: The default value of this mode is "OFF" for the port that includes VMware's Host Group, and is "ON" for the port that does not include VMware's Host Group.			
	2	I	-	None	VB6-0004	Improvement of iSCSI Header / Data digest feature.	Due to good end to end data protection perspective, RSD strongly recommend customer to enable Header and Data Digest feature at initiator/server. DF will follow on this to enable digest for I/O. If it's possible to set both Firmware sets digest enable in iSCSI login sequence.			

	3	C	A	SD3882367	VB6-0005	Controller blockade may occur when Microprogram Error [HDP] is displayed after non-stop firmware replacement.	[Phenomena] The controller blockade occurs with the following Web message when host I/O is received under the conditions of: DP optimization is executed in firmware V8.0/A and later. Incorrect flag is set under the status of DP page address in DF800-EN-M050. After replacing active firmware with V11.5/A and later. HJ4ABX Microprogram error was detected[HDP] The same process occurs in the opposite side afterward and array system goes down. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.5/A (08B5/A) and later [Conditions of Occurrence] The problem occurs certainly when all of the following conditions are met. (1)Incorrect flag is detected in DP page address check tool. (2)Replace non-stop firmware with V11.5/A or V11.5/B firmware. (3)The host I/O is received after non-stop firmware replacement in (2). [Cause] Firmware bug. Array reconstructs DP page address after clearing the flag under migration running status which is incorrectly set at the time of firmware replacement. At this time, reconstruction process is also required for other controllers. ID is issued in order to communicate between controllers and then information is updated. However, in V11.5/A, the ID number of controller communication is used in other process that management information is incorrectly updated and unnecessary process is operated during flag clear process. <Countermeasure> Create separate ID for controllers' communication and operate correctly in flag clear process. [Recovery] Apply the fixed firmware. <Action in the case of the failure> When controller is blockaded, reboot after planned shutdown. When system outage occurs, reboot after power down.
	4	C	B	None	VB6-0003	The chip vendor informed FW defect of 10G iSCSI chip on DKSA2.	[Phenomena] Controller may be blockaded due to a hang-up of DKSA2 10G iSCSI card. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.3/A (08B3/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) When an internal cache error occurs on the iSCSI chip, FW [Cause] Firmware bug. - The cause is the FW defect of the chip. <Countermeasure> - Improve FW routine not to cause cache error. [Recovery] Dummy replacement of the failed controller that installed 10G iSCSI board(DKSA2) <Action in the case of the failure> Apply V11.5/D Firmware or later version after dummy replacement of the failed controller
	5	C	B	None	VB5-0131	When HDD of Unit#0/HDU#0 is not installed, the capacity of 3TB HDD is displayed as "---" and RAID Group/DP Pool cannot be created with 3TB HDDs.	[Phenomena] When HDD of Unit#0, HDU#0 is not installed, the capacity of 3TB HDD is displayed as "---" on HSNM2. In that condition, because 3TB HDDs are not displayed as the candidate of which RAID Group/DP Pool is constituted, RAID Group/DP Pool cannot be created with 3TB HDDs. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.5/A (08B5/A) and later HSNM2 Ver. 11.50 [Conditions of Occurrence] The problem occurs certainly when all of the following conditions are met. (1) Firmware: V11.5/A(08B5/A) and later (2) HSNM2 Ver. 11.50 (3) 3TB SATA HDD (4) The HDD of Unit#0, HDU#0 is not installed. Or an unsupported HDD is installed in the slot of Unit#0, HDU#0.

							[Cause] Firmware bug. The interface logic against HSNM2 has a bug. If the HDD of Unit#0/HDU#0 is not available, 3TB HDD installed in the array is treated as their capacity is zero. <Countermeasure> Install appropriate HDD into Unit#0/HDU#0 and retry the HSNM2 operation (display drive capacity, Create RAID Group, Create DP Pool etc.). [Recovery] Apply the fixed firmware or the fixed HSNM2. <Action in the case of the failure> Install appropriate HDD into Unit#0, HDU#0 and retry the HSNM2 operation (display drive capacity, Create RAID Group, Create DP Pool etc.).		
	V11.5/F, 08B5/F							10/7/2011	375	None
V11.5/F 08B5/F Base System V11.5/D 08B5/D	1	I	-	SD3870690	VB6-0009	Improvement of I/0 performance when drive is under recovery at RAID1,RAID0, and RAID1+0 configuration.	Since the performance difference between host I/O in the normal status and the drive with under recovery was large, the host I/O performance was improved at the time of drive recovery when the following conditions are met. The followings will be effective when all of (1), (2), (3) conditions are met. (1) SSD, SAS, SAS7.2K drive (2) RAID1, RAID0 or RAID1+0 (3) Drive (correction Copy, Dynamic Sparing or Copy Back) is		
	2	I	-	EUC1322287	VB5-0127	HP-UX 11iv3 Dynamic LUN Expansion(DLE) and Constraction(DLC) functions are	Dynamic LUN Expansion(DLE) and Constraction(DLC) functions supported by HP-UX 11iv3 was improved to perform via online.			
	3	C	A	EUC1446845	VB6-0007	If media error frequently occurs in the drive, the host command response delay continues and host access lost may occur.	[Phenomena] If media error frequently occurs in the drive, the drive is unable to be blockaded at an early stage, the host command response delay will continue and host access lost may occur. <Equipment model / Firmware version> DF800S/M, V3.2/A (0832/A) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) RG configurations are RAID5, RAID6, RAIDl or RAIDl+0. (However, in case of RAID1and RAID1+0, such problems do not occur, unless they are under recovery process.) (2)Execute Random Write from host. (3)Drive Read for parity generation will turn out to be media error. (4)When executing Write command to the Block with the media [Cause] Firmware bug. When media errors occur during the process of Read data from the drive in generating parity, the firmware changes its parity generation method and makes the parity generation by reading data from other drives. And then, although the reassignment would be expected to reoccur at the time of writing data to the block which caused media error, the reassignment did not occur when the write in terminates normally without media errors, and the reassignment value is in the state of non count-up. In the result, the drive can not be blockaded at early stage, and the command response delay by frequent media errors continues. For these reasons the host access lost may possibly occur. <Countermeasure> When Read status from the drive in the parity generation shows media error, the reassignment threshold will be count-up by executing the reassignment of the target block. [Recovery] None <Action in the case of the failure> Start the dynamic sparing manually to the drives where media errors		

	4	C	A	None	VB6-0011	Either controller blockade or system down occurs when splitting pairs in a CTG including SI(S)-SS(P) cascade configuration.	[Phenomena] The following two phenomenon may occur when splitting SI pairs under the PAIR/PAIR(IS)/COPY status using the Consistency Group (abbr. CTG) including ShadowImage (abbr. SI) - Snapshot(abbr.SS) cascade configurations, depending on the CTG configurations and type of models. 1. When the occurrence conditions are met in the models other than DF800(EH), a controller will be blockaded with HF0107 Data transfer check error[CCPLUNERR] message. 2. When DF800H(EH) is used or when there are pairs other than SI-SS cascade in a CTG for the other models, if the occurrence conditions are met, the subsystem down occurs with HF0107 Data transfer check error[CCPLUNERR] message. <Equipment model / Firmware version> DF800S/M/H V11.0/A (08B0/A) and later DF800ES/EM/EH, V11.0/A (08B0/A) and later [Conditions of Occurrence] The phenomenon 1 and 2 will appear when the following conditions are met. 1. Controller blockade(Can occur in the models other than DF800H(EH)) (1) Firmware Ver:08B0/A and later (After support version of SI-SS cascade configuration.) (2) SI is enabled. (3) SS is enabled. (4) SI(S)-SS(P) cascade configurations(shared by SI S-VOL and [Cause] Firmware bug. Exclusive control omission for write process at the split of pairs using the CTG. Among the pairs defined in a CTG, only a representative pair is placed within the range of exclusive process. For this reason, the pairs out of the range of exclusive process chnage their status asynchronously and either a controller blockade or subsystem down occurs depending on the timing of write to P-VOL/S-VOL. <Countermeasure> By placing SI pairs within the range of exclusive process, the modification was made to include SI pair within the range of exclusive process, and exclusive process was designed to take place for all the SI pairs in CTG indicated by a split command. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform the procedure subject to the following conditions. (1) When a controller is blockaded. Dummy-replace the blockaded controller. (2)When system was down. Perform OFF/ON on the failed array.
	5	C	A	EUC1469925	VB6-0014	When DP optimization is executed, Microprogramerror[HDP] occurs and controller is blockaded.	[Phenomena] When DP optimization is executed in the condition that there are incorrect pages in DP page address, Microprogramerror[HDP] occurs and the controller will be blockaded. System goes down if the same trouble occurs at the controller of the opposite side afterward. Web message HJ4A9E Microprogram error was detected[HDP](CTL-x) <Equipment model / Firmware version> DF800S/M/H, V8.0/A (0880/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when the operation of (7) is performed after (1)~(6) conditions are met. (1) Using Hitachi Dynamic Provisioning functions. (2) Performing DP optimization (Example adding a DP pool capacity, LU shrink, DP Optimization by manual.) (3) DP Optimization was cancelled via Hitachi Storage Navigator Modular 2 (abbr. HSNM2), or skipped due to migration timeout cause by a heavy write command from a host. One of the following (4)~(5) is executed while (1)-(3)'s conditions are met. (4) Planned shutdown. (5) Firmware is exchanged for the unsupported firmware of DF800-EN-M050. (6) Firmware of V9.0/A and later is installed via fixed

							[Cause] Firmware bug. Because incorrect information is used as a parameter when DP optimization is executed under the incorrect condition of DP address page. <Countermeasure> If incorrect information was given as a parameter, disregard that page and use another page. [Recovery] Apply fixed firmware. <Action in the case of the failure> (1) When controller is blockaded, stop DP optimization immediately and apply fixed firmware after recovering controller. And then, perform planned shutdown and reboot an array and restart DP optimization afterward. (2) When the system is downed, apply fixed firmware during OFF
	6	C	A	EUC1469925	VB6-0013	Controller is blockaded when Microprogramerror[HDP] occurs by host I/O execution after performing power cycle during the process of DP optimization.	[Phenomena] When the host I/0, LU operation process, or DP pool operation process are executed after performing power cycle during the process of DP optimization, DP page address detects contradiction and controller may be blockaded in Microprogram error[HDP]. The system goes down if the same problem occurs at the controller of the opposite side also occurred afterward. Web message HJ4Axx Microprogram error was detected[HDP](CTL-y)(xx: code, y:CTL#(0-1)) HJ11xx Microprogram error[RCH] (xx: code) H900320 Watch-dog time-out I6GU00 R/W command for the LUN is rejected due to invalid LUN process of array(LU-x,y) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.3/E (0893/E) and later [Conditions of Occurrence] The problem occurs certainly when the following condition (1) or (2) is met. (1)Perform power cycle during DP optimization.
							[Cause] Firmware bug. The page information is also updated with the reconstruction process of DP page address at the time of performing power cycle when DP page queue is registered. However, DP page queue was destructed since the page information was incorrectly updated with old information after page queue information was registered. <Countermeasure> The page information is not updated after DP page queue registration process was performed at the reconstruction process of DP page address. [Recovery] Apply the fixed firmware. <Action in the case of the failure> (1) The following message is displayed, but the status of disk array unit is Ready. I6GU00 R/W command for the LUN is rejected due to invalid LUN process of array(LU-x,y) Please perform planned shutdown and reboot an array. (2) If controller is blockaded with the following messages: HJ4Axx Microprogram error was detected[HDP](CTL-y)(xx: code, y:CTL#(0-1)) HJ11xx Microprogram error[RCH] (xx: code) H900320 Watch-dog time-out Please perform planned shutdown and reboot an array after recovering the blockaded controller.
	7	C	B	EUC1448856	VB6-0008	If the firmware version is downgraded from V11.0/A and later to V10.X and before, SATA Write & Compare mode cannot be changed.	[Phenomena] If the firmware version is downgraded from V11.0/A and later to V10.X and before, SATA Write & Compare mode cannot be changed. HSNM2 message "DMES052600:The process failed due to an invalid parameter. Confirm the specified value." <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.0/A(08B0/A) and later [Conditions of Occurrence] The problem occurs certainly when all of the following conditions are met. (1)Use SATA drive (2)Initial setup with the firmware V11.0/A and later (including Configuration Clear Mode) (3)Downgrade the firmware version to V10.X and before (forced downgrade execution)

							[Cause] Firmware bug. SATA Write & Compare mode setting is done by issuing Page35H of Mode Select command from HSNM2. First, HSNM2 reads the page35H that DF firmware retains, then merges only the setting values part of SATA Write & Compare mode, and issues the merged Page35H to the DF firmware by ModeSelect command. The DF firmware, after having received the ModeSelect command, will check the value of Page reserved area as the zero. Whereas the area assigned as the reserved in the firmware of version V10.X and before, the value other than zero is set as default in the firmware of version V11.0/A and later, therefore reserve check will be triggered when it is downgraded to version V10.X and before. Thus, ModeSelect command fails to execute and SATA Write & Compare mode cannot be set.The target area with reserved area's value other than zero is the area which is unable to change setting from HSNM2 even if the firmware is version V11.0/A and later, and the target area cannot be initialized as zero before downgrading, even if it is installed with the firmware of version V11.0/A and later. <Countermeasure> The default value of reserved area be set as zero so that the reserve check should not be executed after downgrading. [Recovery] None <Action in the case of the failure>
	8	C	B	None	VB6-0006	When other backend path check is executed in other path while the backend check is ongoing, incorrect blockade may occur or inappropriate suspected site may be displayed in the web message.	[Phenomena] When other backend path check is executed while the backend check is ongoing, incorrect blockade may occur or inappropriate suspected site may be displayed in the web message. <Equipment model / Firmware version> DF800S/M/H,V7.0/A(0870/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem occurs certainly when all of the following conditions are met. (1)Execute backend diagnosis (2)The execution of backend path check in the path other than (1), while executing (1). Web message The search for the failure part of backend route error started(Path- [Cause] Firmware bug. When another backend check is started in other path while the backend check is ongoing, incorrect blockade may occur or inappropriate suspected part may be displayed in the web messages, since the backend check is executed in reference with incorrect value. Web message Suspected failure part has been detected(CTL-X) Suspected failure part has been detected(Unit-XX, ENC-Y) Suspected failure part has been detected(Unit-XX, HDU-YY) Backend link error was detected(Unit-X, ENC-Y) Backend link error was detected(CTL-Y) <Countermeasure> Modification was made not to refer incorrect values. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform maintenance and replacement service in accordance with web messages. When backend diagnosis is re-executed after maintenance and part replacement service, please perform the service in accordance with
	9	C	B	None	VB6-0001 VB5-0134	HDD may be blockaded at the early stage when Head Diagnosis errors occur in SED.	[Phenomena] HDD may be blockaded without appropriate recovery process when Head Diagnosis errors occur in SED. <Equipment model / Firmware version> For HDD firmware ANH600(S)/ANH600X(S), 5CE2 and later For Array firmware DF800S/M/H, V10.0/B(08A0/B) and later DF800ES/EM/EH, V10.0/B(08A0/B) and later [Conditions of Occurrence] The problem occurs certainly when all of the following conditions are met. (1) Head Diagnosis errors in SED occur intermittently.

							[Cause] Firmware bug. When SED detects Head Diagnosis error, it is reported to the firmware of disk array. If the error exceeds error threshold values(twice/day) managed by a disk array, the drive was blockaded with executing dynamic sparing so that it may be blockaded at early stage. <Countermeasure> The firmware was modified to execute dynamic sparing when it detects error of Head Diagnosis in SED for the 5 times a day. And also, HDD firmware was supported when errors of Head Diagnosis in SED are detected for 5 times a day. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Replace the blockaded HDD.			
	10	C	C	None	VB6-0010	Collection time delay of full dump and simple trace when HDP is locked in the maintenance mode.	[Phenomena] When full dump or simple trace collection is performed after rebooting while HDP priced key locked(or disabled), collecting time will be longer than usual. <Equipment model / Firmware version> DF800S/M/H V7.0/A (0870/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem occurs certainly when all of the following conditions are met. (1) Lock or disable Dynamic Provisioning (2) Disk array system has never been rebooted after the array in (1) became Ready status. (3) Move to maintenance mode. [Cause] Firmware bug. When HDP is locked in full dump or simple trace collection process, it is designed not to collect information from HDP area. However, since the misjudgment will happen at the time of HDP key lock rebooting that it is unlocked and it will tend to collect unnecessary HDP information, it will result in taking a longer time of completing information gathering . <Countermeasure> The judgment logic used at the time of HDP key lock rebooting was modified in order to avoid misjudgment. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Execute Go TO Normal Mode from the maintenance mode.			
	V11.5/H, 08B5/H							10/19/2011	381	None
V11.5/H 08B5/H Base System V11.5/F 08B5/F	1	C	A	EUC1476241	VB6-0017	Host access lost or PIN over may occur when IO is infinitely retried on the drive after controller is blockaded.	[Phenomena] When the drive is replaced after the maintenance service while an old firmware in use and the firmware is updated afterward, controller blockade or reboot type firmware exchange will result in the condition that internal drive of the disk array system cannot be used. The following case 1 or 2 phenomenon may occur, depending on the drive, either a data store or a spare drive. [Case1] With the drive which stores the data, write process to the target drive will not be completed. The write data continues to be stored in the cache so that host access lost may occur by the inflow restriction from the host or PIN threshold may be exceeded. [Case2] In the spare drive, when recovery operation to the spare drive is executed by other drive's blockade, the recovery data continues to be stored in the cache. The host access lost may occur or PIN threshold may be exceeded. <Equipment model / Firmware version> DF800S/M/H, V5.0/A (0850/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Configuration of Dual controller (2) Firmware version is from V3.2/E to V4.6/B. (3) Any of SAS/SATA drives of HDU8~HDU14 in the basic			

							[Cause] Firmware bug. There is a defect in the state management of drive in the firmware version from V3.2/E to V4.6/B, however, changing the diagnosis method of drive in V5.0/A made this defect detectable. With V5.0/A and later, when the process is taken over to the other controller at the time of controller blockade,the already recovered drive was made unusable on state management of drive due to the firmware bug.Since the drive in the configuration information is normal, IO request continues, and the condition which the write data in the cache cannot be outflow continues. Then inflow of data will be restricted or PIN threshold will be exceeded. <Countermeasure> Fix the logic for state management of drive, not to make the drive already recovered unsusable when the process is taken over to the other controller at the time of controller blockade. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform planned shutdown. When planned shutdown is failed with "PS OFF failed" message and if "PIN is over" message is displayed, write data cannot be written to the drive from cache. In such case, execute power OFF and reboot again. Write data can be written to the drive when power OFF/ON is executed. Thus, repeat the action of power OFF/ON two to three times until			
	V11.5/K, 08B5/K							11/18/2011	384	None
V11.5/K 08B5/K Base System V11.5/H 08B5/H	1	C	A	SD4055718	VB5-0138	Controller is blockaded due to attempting the incorrect CPU Load Reduction for Cross-CTL I/O mode default.	[Phenomena] Controller may be blockaded while high-workload host I/O is executing. <Equipment model / Firmware version> DF800/H, VB.0/C (08B0/C) and later [Conditions of Occurrence] The problem may occur when the following conditions are met. (1)DF800H (2)Fibre Channel interface (3)One of the following conditions ((3-1), (3-2) (3-3) or (3-4)) is met. (3-1)DF800H is connected by USP_V/VM's Universal Volume Manager function. (3-2)When the array will be used in high workload conditions. (3-3)When simultaneous commands are more than 4. (3-4) Host connection environment that alternation passing software of Active/Active type works in round-robin fashion. For example: Hitachi Dynamic Link Manager, VxVM-DMP, SUN Traffic Manager etc. [Probability of failure] Low [Cause] Firmware bug. CPU Load Reduction for Cross-CTL I/O mode could not be operated since misjudgment was made when performing CPU Load Reduction for Cross-CTL I/O mode on default. <Countermeasure> Modification for judgment is made for correct default operation of CPU Load Reduction for Cross-CTL I/O mode. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy-replace the blockaded controller. <Web Message> H06J0X [DCTL]The unexpected completion was			
	2	C	A	EUC1487707	VB5-0140	DP optimization is incorrectly operated at the time of DP pool capacity depletion.	[Phenomena] Although DP optimization was performed toward virtual LU which became host inaccessible due to the DP pool capacity depletion, reclaimable capacity would not be shown as actual reclaimed volume. <Equipment model / Firmware version> DF800S/M/H, V8.0/A (0880/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) The condition of DP pool is depleted. (2) The virtual LU will be inaccessible by the cause of data access more than DP pool capacity. (3) Perform DP optimization for inaccessible virtual LU while the condition of DP pool depletion is not released*1. *1 The condition where depletion condition of DP pool is released. <The case of the firmware version older than 08B5/A> The usage capacity of DP pool is less than 95% of entire capacity. <The case of the firmware version 08B5/A or later > The case that DP pool capacity is more than 2TB(the large capacity of DP pool): free space is more than 100GB. The case that DP pool capacity is less than 2TB: The usage capacity of DP pool is less than 95% of DP pool capacity.			

							[Cause] Firmware bug. If DP pool is in depletion condition when DP optimization is performed, the page transfer processing of DP optimization will be skipped due to firmware bug. <Countermeasure> Modification be made so that the page transfer processing of DP optimization will not be skipped even if DP pool is in depletion condition. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform DP optimization, after the depletion condition of DP pool is released*1 by performing one or more of the following measures. (1)Expand the DP pool. (2)Perform to delete 0 data for an inaccessible virtual LU or other virtual LU in DP pool. (3)Perform either deletion, format or reduction of the other virtual LU in DP pool. *1 The condition where depletion condition of DP pool is released. <The case of the firmware version older than 08B5/A> The usage capacity of DP pool is less than 95% of entire capacity. <The case of the firmware version 08B5/A or later > The case that DP pool capacity is more than 2TB(the large
	3	C	A	SD4057142	VB5-139	Controller blockade by firmware exchange at the time filled with many virtual LUs when DP Depletion Detail Reply mode is ON.	[Phenomena] Non-stop firmware exchange will fail by controller being blockaded when non-stop firmware exchange is performed. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.7/A (0897/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1)Mapping mode is enabled. (2)Dynamic Provisioning is enabled. (3)DP pool is existed. (4)(Number of virtual LU in the system) x (login numbers(PORT/CTL) correlated with host group) = more than 35,000 For example:2693(Number of virtual LU in the system) x 16(login numbers) =43,088 >35,000 (5)There is a host group that the DP Depletion Detail Reply mode is effective. [Cause] Firmware bug. Regarding the specification which deletes the status of DP Depletion Detail Reply at the time of non-stop firmware exchange, consolidated resource timeout will occur because of the time consumed by improper loop linkage of the delete object search process. <Countermeasure> Correct modification should be made on the number of loop processing times which deletes the status of DP Depletion Detail Reply at the time of non-stop firmware exchange. Apply the fixed firmware. <Action in the case of the failure> Recover the blockaded controller by dummy replacing. After recovery, turn off all DP depletion detail reply modes and re-perform non-stop firmware exchange. And then, turn ON DP depletion detail reply mode once again after non-stop firmware exchange is completed.
	4	C	A	EUC1477319	VB6-0021	Controller blockade occurs with "Host transfer DMA error was over the threshold" message.	[Phenomena] Controller blockade occurs with the message of "Host transfer DMA error was over the threshold" due to the path failure at SAN IF side. <Equipment model / Firmware version> DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1)FC 8Gbps I/F on board in DF800E. (2)FC path failure occurs and Frame Timeout /Bad AL_PA is detected by FC protocol chip. (3) PCI address error is detected at DCTL. [Probability of failure]

							[Cause] Firmware bug. When the errata of FC protocol chip which the same PCI address is read twice at the time of detection of Frame Timeout / Bad AL-PA occurs and the DCTL failure (PCI address error) is detected, the CTL blockade will occur by incorrect threshold count where it would be supposed to function not to increase the DCTL failed threshold count. <Countermeasure> When PCI address error occurs at DCTL side and errata at FC protocol chip is occurring, set not to raise the DCTL failure counter level. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy-replace the controller after re-examining FC path. <Web Message> HD2100 Host transfer DMA error was over the threshold(CTL-
	5	C	B	None	VB5-0137	Incorrect error occurs when array system is operated by using RAID Manager.	[Phenomena] When the multiple instances of RAID managers are simultaneously booted, command of RAID manager may not be executed by the occurrence of improper error at the time of operation using RAID manager. The following message will be displayed when command execution is failed. <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1)Using RAID Manager (The problem does not occur in Hitachi Storage Navigator Modular 2(hereafter HSNM2)) (2)One of either ShadowImage(SI), SnapShot(SS), TrueCopy(TC), TrueCopy Extended Distance(TCE), Modular Volume Migration(MVM) or Data Retention Utility(DRU) is effective. (3)Multiple RAID manager instances are simultaneously booted. (4)Command device is separated into both controllers by multiple RAID manager instances. (5) A demand on allocating of identifier has failed. (6)Executing following RAID Manager command. pairdisplay,raidscan,pairevtwait,pairsyncwait,pairmon,pairvolchk,paircurchk,raidar,raidvchkdsp,raidvchkscan,paircreate,pairsplit,pairresync,horctakeover,raidvchkset [Cause] Firmware bug. RAID Manager controls multiple instances by allocating an identifier per instance. However, when RAID Managers are simultaneously booted, other information will be overwritten by the registration process of identifier, for each controller detects an identical identifier as search process of free identifier is not excluded. If RAID Manager command is executed under such conditions, command will fail by information inconsistency of instance. <Countermeasure> In the process of allocating the registration of identifier per instance, modification should be made to execute the exclusion of those from search of free identifier up to completion of registration. Apply the fixed firmware. <Action in the case of the failure>
	6	C	C	None	VB5-0142	Unchangeable of a defined virtual LU into Accelerated Wide Striping Mode.	[Phenomena] When a defined virtual LU is made to change the Accelerated Wide Striping Mode effective, the change is guarded with a following HSNM2 message despite of not exceeding the over provisioning threshold value. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.5/A (08B5/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1)Dynamic Provisioning is enabled. (2)Multiple DP pools are defined. (3)Total of a defined capacity of virtual LU of whole DP pool is larger than the capacity to be defined by over provisioning threshold of each DP pool(limited threshold value). (4)Defined virtual LU is made to change the Accelerated Wide Striping Mode [Probability of failure]

							[Cause] Firmware bug. In the process of virtualized excess judgment of DP pool at the time of making effective the wide stripping mode, the initialization of variables to calculate the total of defined capacity of virtual LU by DP pool was missing. With this reason, when more than one DP pool exist, the defined capacity of virtual LU in other DP pool are added and then the virtualized excess value will be judged larger than the actual value. <Countermeasure> Initialize the total value of defined capacity of virtual LU by each DP pool. Apply the fixed firmware. <Action in the case of the failure> Change the Accelerated Wide Striping Mode after applying fixed firmware.		
	V11.5/N, 08B5/N							1/20/2012	388	None
V11.5/N 08B5/N Base System V11.5/K 08B5/K	1	C	A	SD4167156	VB6-0028	Remote array may go down when Swap Pair or horctakeover is performed on TCE volume on Vmware.	[Phenomena] When Swap Pair or horctakeover is performed of TrueCopy Extended Distance (TCE) on an array connecting to VMware ESX(Note 1), "HJ2DA1 Microprogram error[SNR]" may occur on both controllers which leads to system down. Note 1: Target versions: VMware ESX 4.1 and 5.0 <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.3/A (0893/A) and later [Conditions of Occurrence] The problem occurs certainly when all of the following conditions are met. (a-1) Using HSNM2 (1) TCE is enabled. (2) Swap Pair is performed on a TCE pair in Paired status. (3) The pair status of the TCE S-VOL is Busy. (4) A vStorage command is issued to the TCE S-VOL. (a-2) Using CCI (1) TCE is enabled. (2) A horctakeover is performed on a TCE pair in PAIR status. (3) The pair status of the TCE S-VOL is SSWS (Note 3). (4) A vStorage command is issued to the TCE S-VOL. Note 3: When the pair status changes to SSWS, the determined data at the end of the previous cycle is restored to the S-VOL but after the restore process, the pair status does not change from SSWS. Although this phenomenon occurs when the pair status is [Cause] Firmware bug When an S-VOL of TCE accepts Swap Pair or horctakeover, the determined data at the end of the previous cycle needs to be restored to the S-VOL because the data of a TCE S-VOL transfers to the remote array asynchronously. At that time, if the remote array receives a vStorage command (Note 2) from the VMware ESX, the restore process is performed on the area that the vStorage command targets. When an inappropriate LUN is set to a parameter for the restore process due to the firmware bug and is referred to during pair status check, a controller fails because .the pair status is determined inappropriate. Subsequently, the other controller will take over the restore process but the same phenomena occur on the controller, which leads to system down. Note 2: vStorage command includes ATS, XCOPY, WriteSame and Unmap. <Countermeasure> The parameter value of LUN is correctly modified to be set in the restore process that operates at the time of receiving vStorage command. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Disconnect the VMware ESX server from the array, and perform PS OFF/ON so the array reboots. After the array has rebooted, the			

	2	C	A	SD4087668	VB6-0024	Array system down may occur at the firmware update at the array system with SATA drive installed.	[Phenomena] When the firmware is updated at the array system with SATA drive installed, both controllers will be blockaded due to SAS controller failure and array system may go down. <Web Message> HH8U0x D-SPC detected firmware error(CTL-x) <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H,V4.0/A(0840/A)and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) SATA drives are installed. (2) One of the following operations is executed. Or backend failure occurs. -Firmware update -Starting array system -Rebooting array system -ENC replacement -ENC firmware update -Controller replacement -SATA drive replacement -Adding a additional unit with SATA drive installed (3) In (2), linkup sequence between ENC and SATA drive fails due to SATA drive failure. [Cause] Firmware bug When SAS controller returns an error response at the time of drive access, regardless of the error caused by linkup sequence failure due to SATA drive failure, controller will be incorrectly blockaded as SAS controller failure. Another controller will be blockaded in the same way by the retry of drive access and array system down occurs. <Countermeasure> The functionality of searching for the failure part in either SAS controller or SATA drive is improved. When error response is returned from SAS controller if linkup sequence failure occurs, the firmware blockades a SATA drive. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform PS OFF/ON of array system. When the array system does not start, please contact RSD. <Web Message>
	3	C	A	EUC1517163	VB6-0027	Host access lost may occur when online firmware update is executed from HSNM2.	[Phenomena] When online firmware update is executed from HSNM2, host I/Os will not be processed for about five minutes and host access lost may occur. <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H,V4.0/A(0840/A)and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Online firmware update is executed from HSNM2. (2) When controller rebooting starts by online firmware update of (1), LAN data transfer error or transfer delay occurs due to LAN failure with connection of reboot controller. [Probability of failure] Low

							[Cause] Firmware bug When exclusive process is executed in order to start rebooting at the time of controller reboot by online firmware update, and if LAN data transfer latency occurs and LAN data transfer has not completed due to LAN failure, host access lost may occur because exclusive process will not be completed until session timeout(5 minutes) and host I/O processes will be inhibited due to failure. <Countermeasure> When LAN data transfer latency occurs and LAN data transfer has not completed, exclusive processes should be completed after 9 seconds and host I/O processes will be made to execute. [Recovery] Apply the fixed firmware. <Action in the case of the failure> (1)Recover LAN failure, and then reconnect HSNM2 with array system. (2)Re-execute online firmware update "Transfer and update Firmware". (3)If "DMES059510 : The process cannot be performed because the firmware is being replaced." is displayed while executing step(2) and online firmware update fails, check "Update Firmware" of radio button and then update firmware once again.			
	4	C	A	SD4150965	VB6-0025	Controller blockade may repeatedly occur due to the hardware failure of WEB message "The PCI Express device error was detected" at the time of 1Gbps iSCSI interface configuration.	[Phenomena] When host of not mapping to a host group is connected at the time of 1Gbps iSCSI interface configuration, controller blockade may repeatedly occur due to the hardware failure. <Web Message> H09601 The PCI Express device error was detected <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.5/A (08B5/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) 1Gbps iSCSI interface is installed. (2) Firmware version 08B5/A and later. (3) Login and logout to iSCSI target repeatedly occur. (For example, it occurs when the host of not mapping to a host group is connected.) [Probability of failure] Low <Explanation> Subject to occurrence conditions (3), it appears only when System [Cause] Firmware bug When System Error of iSCSI chip occurs, log of iSCSI chip is collected and iSCSI chip will be recovered. However, in 1Gbps iSCSI interface configuration, at the time of log collection, hard error occurs and controller will be blockaded since register access of 10Gbps iSCSI chip toward 1Gbps iSCSI chip is incorrectly executed. <Countermeasure> When 1Gbps iSCSI interface is installed, log of 1Gbps iSCSI interface is correctly collected. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform the dummy replacement for the blockaded controller. Check and make sure if the host of not mapping to a host group is not connected. Disconnect the connected host if there is any case of host connection.			
	V11.7/A, 08B7/A							2/29/2012	390	None
V11.7/A 08B7/A Base System V11.5/N 08B5/N	1	N	-	-	VB8-0001	TrueCopy remote replication between DF800XS/S/M/H/ES/EM/EH and DF850XS/S/MH	TrueCopy remote replication between DF800XS/S/M/H/ES/EM/EH and DF850XS/S/MH is supported. The followings are required. - DF800 firmware Ver.08B7/A and later - RAID Manager Ver. 01-27-03/02 and later - DF800 Maintenance Manual Rev.38 and later - Command Control Interface (CCI) Installation Guide 15th edition and later - Command Control Interface (CCI) Reference Guide 22nd edition and later - Command Control Interface (CCI) User's Guide 22nd edition and later - TrueCopy remote replication User's Guide 21st edition and later - DF850 firmware Ver.0915/B and later, and Hitachi Storage Navigator Modular 2 Ver.21.50 and later			

	2	I	-	-	VB8-0019	Improvement of recovery processes for consecutive media errors of a drive	Recovery processes for consecutive media errors of a drive take a long time and I/O accesses to the drive are inhibited during the processes, therefore host accesses to the drive are affected even if the area where frequent media errors occur is unrelated with host accesses. So the processes are executed at fixed intervals in order not to be affected for host accesses.
	3	I	-	-	VB8-0033	Improvement of simple trace collecting function on the maintenance web	The messages which are displayed at the time of getting trace files are changed, that is to alert the user to click "continue" to get whole trace files. <Before> (i) Just before downloading a file: "Do not close a window until the Trace file output is completed." (ii) Just after downloading a file: "Do not close a window until the Trace file output is completed." <After> (i) Just before downloading a file: "Do not close this window, otherwise you can not get the entire simple trace. The simple trace is composed of one or more files. Please click Download." (ii) Just after downloading a file: "Do not close this window, otherwise you can not get the entire simple trace. You have saved part N of a divided simple trace and subsequent trace files are coming. Please click Continue."
	4	I	-	EUC1525085	VB8-0044	Improvement on remote copy when the remote array is busy	When a write is executed on the P-VOL of TrueCopy remote replication, the write data is copied to the S-VOL at the remote array so the P-VOL and S-VOL become identical. There were cases where the copy to the S-VOL was improperly suspended for a long time while the remote array was very busy with workloads. By modifying the priority of copy to the S-VOL, this improvement prevents the copy from being suspended for a long time even while the remote array is busy.
	5	I	-	-	VB8-0024	Support of ShadowImage Quick operation in a ShadowImage(S-VOL)-TrueCopy(P-VOL) configuration	In the ShadowImage(S-VOL)-TrueCopy(P-VOL) configuration where the S-VOL of ShadowImage in-system replication is cascaded with the P-VOL of TrueCopy remote replication, you can now perform the split and resync operations to the ShadowImage pair in the quick mode.
	6	I	-	-	VB8-0008	Support of the SNMP Trap issued from the dynamic port	The Trap of SNMP is usually issued from 161st port, however, when [SEND ALL TRAPS FROM DYNAMIC PORT] is added to the setting of SNMP (ENV file), Trap will be issued from the dynamic port which has one of the port numbers from 49152 to 65535.
	7	C	A	-	VB8-0053	The S-VOL of TrueCopy remote replication (TC) becomes unavailable for write after pair swap.	[Phenomena] When pair swap is performed while a failure like remote path failure is happening, the S-VOL pair status changes to Takeover. At this time, if the S-VOL receives a write command from the host, the write operation fails improperly. <Web Message> None <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H,V4.0/A(0840/A)and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem occurs certainly when all of the following conditions are met. (1) TrueCopy remote replication is enabled. (2) Any of the conditions indicated in (*1) is met. (The condition (2) is necessary for the condition (4) to be met (Status changes to Takeover) following the condition (3).) (3) Pair Swap is performed by Hitachi Storage Navigator Modular 2(HSNM2) on the remote array. (4) The S-VOL pair status changes to Takeover. At this time, if the S-VOL receives a write command, the write operation fails (*2). (*1) (a) Both of the two remote paths fail.

							[Cause] Firmware bug When Pair Swap is operated, the S-VOL set unavailable for Write, although it must have been set available for Read/Write. <Countermeasure> The firmware is fixed so the S-VOL will be set available for Read/Write when Pair Swap is operated. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform one of the following procedures of (a), (b) and (c). (a) When this problem is happening due to failed remote path, recover the remote path and then perform pair swap operation again. (b) Delete the TC pair. (c) On CCI (RAID Manager), perform pair split operation with the -rb option. <Web Message> None
	8	C	B	-	VB8-0022	Countermeasure for the vulnerability of OpenSSL (CVE-2008-7270, CVE-2010-4180, and CVE-2009-3555)	[Phenomena] When the array and the management software (Hitachi Storage Navigator Modular 2(HSNM2) etc.) are in the process of performing the secure communication (authentication and encrypted communication by SSL), the third party could attack the vulnerability of OpenSSL and change the encrypted algorithm used for communication to a weak encryption level algorithm. The vulnerability is open to the public as CVE-2008-7270, CVE-2010-4180, and CVE-2009-3555. <Web Message> None <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H,V4.0/A(0840/A)and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when either (1) or (2) of the following conditions is met. (1) Using SSL The secure communication is selected in the communication between management software such as HSNM2 and the array. (2) Using the maintenance Web Https is used to access from Web browser to Web server of the array (secure communication is performed with the access to the Web server by this process). [Cause] Firmware bug The vulnerability was found in the OpenSSL library of the firmware. The encrypted algorithm used for communication may be changed to a weak encryption level algorithm due to the vulnerability. <Countermeasure> The patch for the vulnerability described above is applied to the Open SSL library of the firmware. By this step, the weak encryption level algorithm will not be illegally changed. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Apply the fixed firmware. <Web Message> None

	9	C	C	-	VB8-0023	After obtaining IP address in DHCP, IP address displayed in Hitachi Storage Navigator Modular 2(HSNM2)/Web will not change.	[Phenomena] In regard to the management LAN port of an array, even though the IP address is obtained in DHCP, IP address displayed in HSNM2/Web may remain the same as before obtaining the address. <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H,V4.0/A(0840/A)and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) DHCP function is enabled. (2) Obtaining IP address by DHCP for the management LAN port (3) ARP packet is continuously received to the port of (2) within 1.5 seconds interval. [Probability of failure] Low <Explanation> The phenomenon occurs certainly if the conditions are met, however, the conditions of continuing to receive ARP packet within 1.5 seconds interval will not usually occur. [Cause] Firmware bug There is a bug in the DHCP process of the network process (=When the network stack receives an ARP packet within 1.5 seconds after obtaining IP address by DHCP, the current IP address information is not updated). <Countermeasure> The modification is made to update the current IP address information in the DHCP process of the network process. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Remove and insert the LAN cable (insert it after an interval of 1.5 seconds or more). <Web Message> None
	10	C	C	-	VB8-0045	When a simple trace is analyzed by TDCONV4, Serial Number of the controller may not be displayed.	[Phenomena] When a simple trace collected from a slave controller (usually it is controller 1) is analyzed by TDCONV4, the value at "CTL0 Serial No." located in <Traceability Display> field of TDCONV4 MESSAGE sheet may not be displayed. <Web Message> None <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H,V4.0/A(0840/A)and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem occurs certainly when all of the following conditions are met. (1) Executing online firmware update (2) The following events have not occurred after (1). -Planned shutdown -Starting the array unit -The controller replacement -The controller automatically reboots after the controller is blockaded, and then it automatically recovers. -updating firmware for each Control Unit one by one stopping the I/O in the dual controller configuration (3) Collecting a simple trace from the slave controller (usually it is

							[Cause] Firmware bug Although the controller's serial number information is initialized at the start of online firmware update, the slave controller (usually it is controller 1) has not obtained the controller serial number from the master controller (usually it is controller 0) at the termination of online firmware update. <Countermeasure> At the time of terminating the online firmware update, the slave controller (usually it is controller 1) obtains controller's serial number from the master controller (usually it is controller 0). [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform either (a) or (b) of the following procedures and Analyze the simple trace by TDCONV4. (a)(1) Apply the fixed firmware or Turn OFF/ON the array system. (2) Collect the simple trace. (b)(1) Collect the simple trace from another controller. <Web Message> None			
	V11.7/B, 08B7/B							4/5/2012	397	None
	V11.7/B, 08B7/B							4/5/2012	397	None
V11.7/B 08B7/B Base System V11.7/A 08B7/A	1	N	-	-	VB8-0041	TrueCopy Extended Distance between DF800S/M/H/ES/EM/EH and DF850XS/S/MH	TrueCopy Extended Distance between DF800S/M/H/ES/EM/EH and DF850XS/S/MH is supported. The followings are required. - DF800 firmware Ver.08B7/B and later - RAID Manager Ver. 01-27-03/02 and later - DF800 Maintenance Manual Rev.39 and later - Command Control Interface (CCI) Installation Guide 15th edition and later - Command Control Interface (CCI) Reference Guide 22nd edition and later - Command Control Interface (CCI) User's Guide 22nd edition and later - TrueCopy Extended Distance User's Guide 19th edition and later - DF850 firmware Ver.0916/A and later, and Hitachi Storage Navigator Modular 2 Ver.21.60 and later			
	2	I	-	SD3628653	VB8-0010	Improvement of failed ENC detection	The ENC firmware is improved to detect the error (No Destination error) of SATA drive address information in the ENC hardware so the array system firmware blockades the failed ENC.			
	3	I	-	SD4314690	VB8-0063	Improvement of failed controller detection	The firmware is improved so that the firmware detects an incorrect access from the other controller with a hardware failure, etc. and does not blockade the normal controller to avoid the array system outage with both controller failures.			
	4	I	-	-	VB8-0064	Improvement of the avoidance of ENC blockade	The ENC firmware is improved so that when a command to the ENC from a controller is aborted due to a controller failure, the ENC firmware discards the command to avoid ENC blockade with ENC firmware processing hang-up.			
	5	I	-	-	VB8-0004	Improvement of drive diagnosis	The failure drive detection is improved to identify a drive with response delays based on the average response time among 3 drives or more of a RAID group to avoid a normal drive blockade.			
	6	I	-	-	VB8-0060	Improvement of backend diagnosis	The backend diagnosis is improved for the firmware not to blockade normal ENC when backend diagnosis does not detect the failed parts due to a controller intermittent error, etc.			
	7	I	-	-	VB8-0027	Improvement of LU format processing	The performance of LU format is improved during high-load host I/Os for RAID1 or RAID1+0 with SAS drives or SSDs.			
	8	I	-	-	VB8-0065	Improvement of Web server security	In order to improve security, the information on the Web server (=HTTP server) of the array is concealed. Concretely, the server identification information in the response messages from the Web server is changed to "XX..XX".			

	9	C	B	SD4307774	VB7-0013	A controller failure may occur with WEB information message "Microprogram error[LSM]" on local side array in TrueCopy remote replication(hereinafter TC) or TrueCopy Extended Distance (hereinafter TCE) configuration via Fibre Channel interface.	[Phenomena] A controller failure may occur on local side array in TC or TCE configuration via Fibre Channel interface. <Web Message> HJ091D Microprogram error[LSM] <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H,V4.0/A(0840/A)and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Fibre Channel interface is installed. (2) TC or TCE is enabled. (3) Remote path is set via Fibre Channel port. (4) More than two TC or TCE pairs are created. (5) The ownerships of LUs of (4) are shared by separate cores (separate controllers in DF800M/S/EM/ES). (6) In the Fibre Channel port of remote path at array on local side, link down/up occurs by pulling out and inserting an optical cable, etc. [Probability of failure] Low <Explanation> [Cause] Firmware bug When the control core (1) of Fibre Channel port operates PLOGI processing due to Link down/up and the reset PLOGI processing is operated from a different core (2) (or a controller) occur simultaneously, PLOGI processing was attempted to operate in duplicate due to the firmware bug and the controller failure occurs. (*1) The reset PLOGI processing is the process that operates with recovery when timeout occurs and ABTS command is issued by the response delay due to Link down/up. <Countermeasure> The modification was made for the reset PLOGI processing so as not to operate when PLOGI processing and reset PLOGI processing occur simultaneously. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy-replace the blockaded controller. <Web Message>
	10	C	B	-	VB8-0058	Controller blockage may occur with the WEB information message "Watch-dog time-out" or "Kernel processing error" during host I/Os.	[Phenomena] When two or more sequential read accesses are being received on one LU, a controller may be blocked. <Web Message> H90320 Watch-dog time-out or HZ0N0x Kernel processing error (CTL-x) <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H,V4.0/A(0840/A)and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The phenomenon may occur when the following (1) to (3) conditions are met and any of (4) to (7) is met. (1) Two or more sequential read accesses are received on one LU. (2) Logical block address (LBA) of each sequential read access of (1) differs by 30 GB or more. (3) The multiplicity of read commands is 6 or more at each sequential read access of (1). (4) Cache segments are depleted due to high-load host I/Os. (5) Cache hit Read is triggered successively by host I/Os. (6) Drive blockage occurs in the RAID group of RAID1 or RAID1+0. (7) Forced Parity Correction procedures are performed after drive blockage occurs in the RAID group of RAID5 or RAID6. [Probability of failure]

							[Cause] When two or more sequential Read accesses are received on one LU, a prefetch JOB operates while switching between the multi stream and single stream modes. However, a prefetch JOB in the multi stream mode may incorrectly overwrite a termination LBA of a prefetch JOB in the single stream mode due to the firmware bug. When the termination LBA is overwritten with a value that is 30 GB or larger than it, the processing of the prefetch JOB will take a longer time and controller blockage will occur because the prefetch JOB reads a wide range of LBA in the single stream mode. <Countermeasure> The modification was made to the prefetch JOB in the multi stream mode so as not to incorrectly overwrite the termination LBA for the prefetch JOB in the single stream mode. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy-replace the blocked controller. <Web Message> H90320 Watch-dog time-out or HZ0N0x Kernel processing error	
	11	C	B	-	VB8-0062	A controller failure may occur with WEB information message "Host transfer DMA error was over the threshold" in TrueCopy remote replication (hereinafter TC) or TrueCopy Extended Distance (hereinafter TCE) configuration via fibre channel 8Gbps interface.	[Phenomena] A controller failure may occur in TC or TCE configuration via fibre channel 8Gbps interface. <Web Message> HD2100 Host transfer DMA error was over the threshold <Equipment model / Firmware version> DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) DF800ES/EM/EH (2) Fibre Channel 8Gbps interface is installed. (3) TC or TCE is enabled. (4) TC or TCE is configured via Fibre Channel port of (2). (5) Intermittent fibre channel failures occur without linkdown at a connected device (Fibre Channel switch or Host bus adapter, etc.) of Fibre Channel port of (2). [Probability of failure] Low <Explanation> The frequency of occurrence is low because the phenomenon appears when the intermittent fibre channel failures occur at the	
	12	C	B	-	VB8-0034	A controller failure may occur with WEB information message "H90320 Watch-dog TimeOut" during host I/O in iSCSI configuration.	[Phenomena] A controller failure may occur during host I/O in iSCSI configuration. <Web Message> H90320 Watch-dog time-out <Equipment model / Firmware version> DF800 S/M/H/ES/EM/EH, V11.5/B (08B5/B) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) iSCSI interface is installed. (2) More than 14 hosts are connected to two ports, port A and B or E and F of a controller. (3) I/Os from all hosts of (2) delay because retransmission of TCP packet(s) frequently occurs due to bad quality of network or backend failure frequently occurs in the array system, etc. [Probability of failure] Low <Explanation> The frequency of occurrence is low because the phenomenon	

							[Cause] Firmware bug Having received a task Management command based on the occurrence condition (3), the firmware will reset host I/Os. However, when having simultaneously received the Task Management commands from 14 hosts or more, Watch-dog time-out will be detected due to the firmware bug that the host I/O reset processing is continuously executed, and the controller failure will occur. <Countermeasure> The modification was made for the reset processing so as not to operate continuously beyond a certain period of time. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy-replace the blockaded controller.	
	13	C	B	-	VB8-0032	When iSCSI information is input with a file using Hitachi Storage Navigator Modular 2 (hereinafter HSNM2), a controller failure may occur with WEB information message "Microprogram error[LSM]".	[Phenomena] When iSCSI information is input with a file using HSNM2, a controller failure may occur. <Web Message> HH7ED4 Microprogram error[ILM] <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.7/A (0897/A) and later [Conditions of Occurrence] The problem occurs certainly when all of the following conditions are met. (1) iSCSI interface is installed. (2) LUN Manager is enabled. (3) More than 176 iSCSI targets are created in one iSCSI port. (4) iSCSI logins are performed on more than 176 iSCSI targets of (3) from host. (5) iSCSI information is input with a file using HSNM2. (More than 176 iSCSI Target Names are changed.) [Probability of failure] High <Explanation> The problem occurs certainly when all of the above conditions are	
	14	C	B	-	VB8-0012	An ENC installed to RKAKS may be blockaded at the first starting of array system or the firmware installation.	[Cause] Firmware bug When there is a login host in the iSCSI port at iSCSI Port Information settings, iSCSI connection with login host is closed once. If the more than 176 iSCSI Target Names are changed at once, the controller failure occurs by misunderstanding that the connection close processing is timed out due to the firmware bug of calculating the connection close processing time. <Countermeasure> The modification was made so as to correctly calculate the connection close processing time. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy-replace the blockaded controller. <Web Message>	
	15	C	B	-	VB8-0012	An ENC installed to RKAKS may be blockaded at the first starting of array system or the firmware installation.	[Phenomena] An ENC installed to RKAKS may be blockaded at the first starting of array system or the firmware installation. <Web Message> I5I200 ENC recovery failed[Linkup NG] W0Fze0 ENC alarm <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.0/A (08B0/A) and later ENC Firmware for 2.5 inch expansion unit, 07-02-13 and later [Conditions of Occurrence] The problem may occur when any one of the following procedures of (1) to (6) is performed and the firmware executes ENC firmware download processing. (1) Starting the array system connected with RKAKS for the first time (*1) (2) Replacing an ENC of RKAKS (*1) (3) Adding RKAKS (*1) (4) A firmware is installed to the array system to which RKAKS is connected. The version of ENC firmware bundled by this array system firmware to be installed is newer than the ENC firmware version of ENC installed to RKAKS. (5) Online ENC firmware download procedures or offline ENC firmware download procedures is performed to the array system	

							[Cause] ENC firmware bug When internal RMA accesses of ENC firmware and ENC hardware conflict at ENC reboot of ENC firmware download, ENC firmware incorrectly detects a parity error due to the ENC firmware bug and ENC blockade occurs. <Countermeasure> The ENC firmware was modified in order not to detect parity error incorrectly at ENC reboot. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy-replace the blockaded ENC. <Web Message> I5I200 ENC recovery failed[Linkup NG]	
	15	C	B	-	VB8-0013	A controller failure or an ENC blockade may occur at the firmware installation or the first starting of array system.	[Phenomena] A controller failure or an ENC blockade may occur at the firmware installation or the first starting of array system. <Web Message> In case that a controller failure occurs HF080x ENC recovery failed[Linkup NG] W01z0x CTL alarm In case that an ENC blockade occurs I5I200 ENC recovery failed[Linkup NG] W0Fze0 ENC alarm <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H,V4.0/A(0840/A)and later DF800ES/EM/EH, V9.0/A (0890/A) and later ENC Firmware for 2.5 inch expansion unit, 07-02-13 and later ENC Firmware for other conventional units, 06-01-12 and later [Conditions of Occurrence] The problem may occur when the array system firmware executes ENC firmware download by any one of the following procedures from (1-1) to (1-9) and the failure of (2) occurs during that time. In case that a controller failure occurs (1-1) Starting the array system for the first time (*1) (1-2) Replacing controller (*1) (1-3) Installing the array firmware [Cause] ENC Firmware bug When ENC firmware returns command status for the ENC reboot command of ENC firmware download to the array system firmware and an intermittent backend path failure occurs, the array system firmware will retry the command. However, the retry command fails and ENC blockade occurs because ENC firmware recognizes those double commands as illegal due to the ENC firmware bug and discards the retry command. <Countermeasure> The ENC firmware was modified so that when ENC firmware receives ENC reboot commands in duplicate, ENC firmware correctly responds the command status for the second command. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy-replace the blockaded ENC or controller. <Web Message> In case that a controller failure occurs HF080x ENC recovery failed[Linkup NG] W01z0x CTL alarm In case that an ENC blockade occurs	

	16	C	B	-	VB8-0011	When the array system is booted up with only one ENC being installed to RKAKS, the other ENC may not recover even if the ENC is inserted in RKAKS.	[Phenomena] When the array system is booted up with only one ENC being installed to RKAKS, the other ENC may not recover even if the ENC is inserted in RKAKS. <Web Message> I5I200 ENC recovery failed[Linkup NG] W0Fze0 ENC alarm <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.0/A (08B0/A) and later ENC Firmware for 2.5 inch expansion unit, 07-02-13 and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) RKAKS is connected. (2) Only one ENC is installed to RKAKS. (3) The other ENC of (2) is inserted in RKAKS after the array system boots up. [Probability of failure] Low <Explanation> The frequency of occurrence is low because the phenomenon [Cause] ENC Firmware bug When the ENC is inserted, Suspending reset signal from installed ENC to the inserted ENC with array system firmware makes the inserted ENC start CUDG processing along with RKAKS access. After the inserted ENC is detected, the installed ENC inhibits the monitoring processing along with RKAKS access for a certain period of time in order to avoid a collision between RKAKS access of inserted ENC and that of installed ENC. However, in the case that the suspend of the reset signal delays due to the load of array system firmware, etc., the recovery of inserted ENC fails because the RKAKS accesses conflict with the CUDG processing of inserted ENC and the monitoring processing of installed ENC. <Countermeasure> The ENC firmware was modified so that when the installed ENC detects the inserted ENC, the ENC firmware of installed ENC immediately suspends the reset signal to the inserted ENC. For this reason, CUDG processing of the inserted ENC will immediately starts so that RKAKS accesses of the inserted ENC and the inserted ENC will not conflict. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy-replace the blockaded ENC.
	17	C	B	-	VB8-0061	When the ENC cable is not connected by work error at the controller replacement or the ENC replacement, the WEB information message will be displayed to confirm if ENC cable is correctly connected at the backend route of the other side of replacement part.	[Phenomena] When the ENC cable is not connected by work error at the controller replacement or the ENC replacement, the WEB information message (1) is supposed to be displayed though WEB information message (2) is displayed, and the service personnel is unable to find unconnected ENC cable. <Web Message> <Web Message (1)> At the controller replacement HH9N0x ENC recovery failed[Cable error] W01z0x CTL alarm At the ENC replacement I5HB00 ENC recovery failed[Cable error] W0Fze0 ENC alarm <Web Message (2)> At the controller replacement HH9Y0x ENC recovery failed[Linkup NG in the other route] W01z0x CTL alarm At the ENC replacement I5JJ00 ENC recovery failed[Linkup NG in the other route] W0Fze0 ENC alarm <Reference> Recovery procedures for "ENC recovery failed[Cable error]". Please make a service personnel confirm if ENC cables are

							[Cause] Firmware bug Linkdown for both backend routes is checked at the replacement of a controller or an ENC. When linkdown caused by the unconnected ENC cable is detected, the WEB information message is always shown indicating that there is unconnected ENC cable at the backend route of the other side of replacement part, due to the firmware bug which does not judge if the linkdown route is at replacement part side or the other side of replacement part. <Countermeasure> The firmware was modified so that the correct WEB information message is displayed by correctly judging the linkdown route. In case that the linkdown route is at replacement part side ENC recovery failed[Cable error] In case that the linkdown route is at the other side of replacement part ENC recovery failed[Linkup NG in the other route] [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform the following procedures. (1) When the following WEB information message is displayed, confirm if the ENC cable is connected to the controller or the ENC which failed to recover. (2) When the ENC cable is not connected, make sure to remove
	18	C	B	-	VB8-0017	In bi-directional TrueCopy (hereinafter TC) configuration, both remote paths are blocked and the status of TC pairs may change to "PSUE".	[Phenomena] In bi-directional TC configuration, when write commands are being received to P-VOLs of TC pairs, both remote paths are blocked and the status of TC pairs may change to "PSUE". <Web Message> W0K0xy Path alarm I90100 Command time out IB1T00 PSUE occurred[TrueCopy] <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H,V4.0/A(0840/A)and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) TC is enabled. (2) Remote paths are bi-directionally connected. (3) Both local side and remote side arrays simultaneously receive write commands (Write commands, ATS commands, WriteSame commands, UNMAP commands, and XCOPY commands) to P-VOL. (*1) (4) In both arrays, any one of the following conditions is met. - Online firmware update is performed. - RAID group expansion is performed. - DP pool is used. - XCOPY command is received to the LU of TC Pair. [Cause] Firmware bug When the occurrence condition (4) is met upon receiving the write command of the occurrence condition (3), both local side and remote side arrays execute exclusive processing. However, write command should be executed even though exclusive processing is in progress in order to avoid dead lock of remote path. Because the write commands cannot be executed due to the firmware bug of exclusive determination of exclusive processing, the both remote paths will be blocked with the occurrence of dead lock of remote path. <Countermeasure> The modification was made for the exclusive determination so as to execute write command during exclusive processing. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Recover the blocked remote paths and perform resynchronization on the TC pairs which were changed to PSUE. <Web Message> W0K0xy Path alarm

	19	C	B	-	VB8-0035	When an optical signal failure occurs in a host connector installed to a 10Gbps iSCSI interface, the blockaded host connector may improperly recover.	[Phenomena] When an optical output signal failure is detected at a host connector installed to a 10Gbps iSCSI interface at the time of array system booting or controller replacement, the host connector blockade occurs once. However, immediately after that, host connector may automatically recover. <Web Message> W0Pz0f Host connector alarm(Portxy) I53A0f Host connector recovered(Portxy) <Equipment model / Firmware version> DF800 S/M/H/ES/EM/EH, V11.5/A (08B5/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) iSCSI 10Gbps interface is installed. (2) Booting the array system or the controller replacement (3) An optical output signal failure is detected at a host connector installed to the interface of (1) at the time of (2). [Probability of failure] Low <Explanation> The frequency of occurrence is low because the phenomenon [Cause] Firmware bug When an optical output signal failure is detected at the host connector during the authentication processing of the host connector at the array system booting or the controller replacement, the host connector blockade processing is executed. However, after that processing, the authentication processing continues due to the firmware bug, and if the authentication processing is successful, the host connector will improperly recover. <Countermeasure> The firmware was modified so that the firmware detects an optical output signal failure after the authentication processing of the host connector finishes. [Recovery] Apply the fixed firmware. <Action in the case of the failure> When two of the following Web information messages are displayed at the array system booting or the controller replacement, replace that host connector. <Web Message>		
	V11.7/D, 08B7/D							4/27/2012	401	None
V11.7/D 08B7/D Base System V11.7/B 08B7/B	1	I	-	SD4277685	VB8-0077	Improvement of system copy processing at media error detection	When system copy fails due to the uncorrected media error (sense code 03/0C03) and system area blockade occurs, online verify processing does not perform reassignment. Because of this, retry of system copy repeatedly fails and system copy does not complete. The firmware is improved that online verify processing performs			
	2	I	-	-	VB8-0070 VB8-0071	Improvement of the controller diagnosis	When an access violation occurred to the other normal controller due to hardware failure of a controller, there is a possibility that the array system goes down by both controllers blockade. The firmware is improved so as to avoid array system down by detecting a hardware failure at early stage and blocking the controller by performing the access violation diagnosis			
	3	I	-	-	VB8-0078	Improvement of path performance in multi path configuration	The firmware is improved to upgrade path performance with host accessing to array from active path in multi path configuration using such as Hitachi Dynamic Link Manager (HDLM) by reporting to the host in addition to Primary/Secondary path information on Inquiry response.			

	4	C	A	SD4324183	VB8-0081	S-VOL data inconsistency or remote path failure occurs on TrueCopy(TC) between DF700 and DF800.	[Phenomena] When resynchronization or swap is performed on a TC pair between DF700 and DF800, the copying completes with differential data remaining on the S-VOL, which results in data inconsistency between the P-VOL and the S-VOL. Or both remote paths failure and PSUE (Failure) of the pairs occur before the copying completes. In both cases, the data of P-VOL is correct. <Web Message> Remote path failure: I90621 RSP illegal request(Key[05],Code[2100]) <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] There are three sets of conditions. < Condition 1> The problem appears when all of the following conditions are met. (1) TC is enabled. (2) DF700XS/S/M/H is connected to DF800S/M/H/ES/EM/EH via remote paths. (3) There is a TC pair that meets the following conditions. -The local array with the TC P-VOL is DF700XS/S/M/H. -The remote array with the TC S-VOL is DF800S/M/H/ES/EM/EH. -The capacity of P-VOL and S-VOL is over 16 GB. [Cause] Firmware bug In the resynchronization/swap logic, the differential bitmaps on the local and remote arrays get merged and the differential data equivalent to the merged differential bitmap is transferred to the S-VOL. The differential bitmaps are merging by 2KB block (referred as 16GB differential data) on DF700. Differential block address is managed by 1 byte on DF700, but differential block address is managed by 2 byte on DF800 and later. In the case of connecting to DF700, differential block address is managed by 2 byte incorrectly on DF800 in spite of having to be managed by 1 byte. Because of this, the wrong differential block is informed to DF700. (Example: address "0x01" on DF700 is treated as address "0x0100" on DF800) <In the case of data inconsistency > When S-VOL in DF800 has differential data, the differential bit in DF800 is settled as 1 (there is differential data). If the differential bit on wrong address referred by this firmware bug is settled as 0, the copying the differential data is not executed and the S-VOL data inconsistency occurs. (The copying is completed with S-VOL differential data remaining) < In the case of both remote paths failure and PSUE (Failure) of the pairs> The differential bitmap is managed by 2KB (referred as 16GB differential data) and every bit for the area outside of the LU is
	5	C	A	SD4378141	VB8-0073	When controller failure occurred during TCE data transfer in TrueCopy Extended Distance (hereinafter TCE) configuration, pair status may change to "PSUE" and then array system down may occur by the blockade of the other controller.	[Phenomena] When pair status is "PAIR " or "COPY" in TCE configuration and if controller failure(A) occurs, the used capacity of data pool may become an incorrect value which improperly exceeds threshold value or less than 0 and accordingly, pair status may change to "PSUE"(*1) or "PFUS". When the used capacity of data pool goes to value less than 0, pair operations except for pair deletion cannot be performed because of error(*2). Even though pair did not change to "PSUE" at controller failure(A), pair operation, user data access to S-VOL, or TCE data transfer triggers pair to change to "PSUE" and controller failure(B)(*3) may occur at the same time. When the latter controller failure (B) occurs before the former blockaded controller (A) recovers, the array system down occurs. <Web Message> (*1) I6D100 Data pool utilization is over the threshold(Data pool-XX) (*2) IB1900 Remote copy failed(CTG-X) (*3) HJ2CQA Microprogram error[POM] or HJ2CQV Microprogram error[POM] <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence]

							[Cause] Firmware bug If controller failure occurs in the process of updating data pool when TCE data transfer switches to next cycle, the firmware calculates used capacity of data pool from non-latest data pool information exclusive for controller, not from data pool information shared by both controllers due to the firmware bug. Accordingly used capacity of data pool will be incorrect and TCE pair and SnapShot pair belonging to data pool may change its(their) status to "PSUE" or "PFUS". Even though pair did not change to "PSUE" at that time, with the data pool access processing by pair operation, user data access to S-VOL or TCE data transfer, TCE pair status changes to "PSUE" and controller failure occurs when incorrect used capacity of data pool is detected. <Countermeasure> The modification was made to firmware so as to calculate the data pool usage after having updated the latest data pool information exclusive for controller. [Recovery] Apply the fixed firmware. <Action in the case of the failure> If the used capacity of data pool has incorrect value which improperly exceeds threshold value or less than 0, perform the following data pool recovery procedures. (1) Delete all SnapShot pair and TCE pair belonging to data pool
	6	C	A	SD4374853	VB8-0074	Host accesses may stop by exceeding the number of PIN data (the write data unable to write on the drive) than threshold value while dynamic sparing of SATA drive is being performed.	[Phenomena] While errors in a SATA drive frequently occur and dynamic sparing processing is performed (*1) and when write commands are received to the LU of that drive, write commands may not be performed because the number of PIN data (write data which cannot be written on the drive) exceeds threshold value (*2). If so, as its result, host accesses stop due to the array system returning the error response (sense code 04/E400) to the host. <Web Message> (*1) I15A00 Dynamic sparing start (Unit-x, HDU-y)[z] (*2) W3M000 PIN is over RAID group threshold[write will not run](DIR-x, RG-y) <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when the condition (6) is met after having met the following conditions (1) to (5). (1) SATA drive (2) RAID1 or RAID1+0 (3) Spare drive is set. (4) Errors frequently occur in the master drive of (2) and dynamic sparing (data recovery processing) starts. (5) Errors continue to occur at the master drive of (2) after (4). (6) Write commands are received. [Cause] Firmware bug When the errors in an original drive of dynamic sparing keep occurring during dynamic sparing, that drive enters into quasi blocked state by the firmware. And also, when an LU of SATA drives receives write command, firmware performs read operation for 512/520 byte conversion. If the original drive configures RAID group of RAID1 or RAID1+0, the firmware should perform read operation on mirror drive. However, since firmware performs read operation on spare drive due to the firmware bug, write command processing is not completed because read operation fails. Received write data becomes PIN data since it cannot be discarded, and upon continued receipt of write command, PIN data is accumulated in the cache memory. As a result, the number of PIN data exceeds the threshold value and write command is unable to be performed. <Countermeasure> The modification was made in order for the firmware to perform read operation correctly on mirror drive for 512/520 byte conversion. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform procedures (1) or (2).

	7	C	A	-	VB8-0084	Linkdown and linkup repeatedly occur at iSCSI port and host accesses may stop.	[Phenomena] Linkdown and linkup repeatedly occur at iSCSI port and host accesses may stop. <Web Message> None <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.7/H (0897/H) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) iSCSI interface is installed. (2) I/Os from multiple hosts (including multiple guest operating systems of VMware) delay in an iSCSI port of (1) because retransmission of TCP packet(s) frequently occurs due to bad quality of network or backend failure frequently occurs in the array system, etc. (3) Condition (2) continuously occurs. [Probability of failure] Low <Explanation> The frequency of occurrence is low because the phenomenon appears when the Task Management commands (LUR command, [Cause] Firmware bug When the firmware receives two or more Task Management commands at the same time, the firmware should abort the earlier received command and release that command resource. However, the firmware may not release the resource due to a bug. If unreleased resources accumulate and the command resources are depleted, the firmware repeats reset of iSCSI port so that linkdown and linkup of iSCSI port repeatedly occur. <Countermeasure> The modification was made on firmware to release the resource on Task Management correctly. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy-replace the controller with the iSCSI port that linkdown and linkup occur repeatedly. <Web Message>
	8	C	A	-	VB8-0076 (same as DF850 V16-0237)	Array goes down when migration of MVM is performed on LUs with different sizes.	[Phenomena] One of the following problems can occur when migration of Modular Volume Migration (hereinafter MVM) is performed on LUs with different sizes. Problem A: Despite different sizes of LUs, migration starts and completes while it is partially copied. Problem B: Despite different sizes of LUs, migration starts and the array goes down after a while. After this, array goes down again even if array is rebooted. <Web Message> Problem A: None Problem B (in case that S-VOL is a normal LU): HF1100 Data transfer check error[WSEGPDEV](CTL-0) HF1101 Data transfer check error[WSEGPDEV](CTL-1) Problem B (in case that S-VOL is a virtual LU): HJ22O0 Microprogram error[CCP] <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem occurs certainly when all of the following conditions are met. (1) MVM is enabled. (2) LUs with different sizes are selected for MVM pair creation.

							[Cause] Firmware bug A firmware is found in a logic of checking the size of an LU for MVM migration. The size of a variable to store an LU size is insufficient and the overflow of the LU size is occured. As a result, it is incorrectly determined that LUs with different sizes have the same size and they may be paired with migration. In such cases, LU LBA outside of the S-VOL are accessed, which results in a CTL failure. Those processes are taken over to the other CTL and the same thing happens on the CTL, which leads to array down. <Countermeasure> Expand the size of the variable to store an LU size in the logic of checking an LU size during MVM pair creation. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Problem A: Specifying the correct LU, execute the migration of MVM again. Problem B: In order to end the migration, volatilize the cache memory and boot the array. Then delete the pair. <Web Message> Problem A: None Problem B (in case that S-VOL is a normal LU): HF1100 Data transfer check error[WSEGPDEV](CTL-0) HF1101 Data transfer check error[WSEGPDEV](CTL-1)			
	9	C	B	-	VB8-0072 (same as DF850 V17-0071)	Controller is blockaded with Web message "Stack Watermark Over alert was detected" when DHCP is set.	[Phenomena] When DHCP is set while SNMP Agent Support Function is enabled, a controller may be blockaded. <Web Message> H0F80x Stack Watermark Over alert was detected (CTL-x) H90210 CTL failure IB1400 SNMP agent detected the error W3Q00x SNMP error occurred in the SNMP function(CTL-x) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.7/A (0897/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) SNMP Agent Support Function is enabled. (2) DHCP is set. (3) By booting DHCP server or connecting LAN cable to user port after starting array system, it obtains IP address from DHCP server. [Probability of failure] High <Explanation> When the conditions of occurrence are met, controller failure [Cause] Firmware bug Although SNMP error occurs according to occurrence condition (3), the program stack size is insufficient to output SNMP error message so that controller failure occurs. <Countermeasure> Increase the program stack size necessary to output SNMP error message. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Recover the controller by dummy replacing blockaded controller. <Web Message> H0F80x Stack Watermark Over alert was detected			
	V11.7/E, 08B7/E							5/11/2012	406	None

V11.7/E 08B7/E Base System V11.7/D 08B7/D	1	C	B	EUC1564770	VB8-0093	A controller failure may repeatedly occur on local side array in TrueCopy remote replication (hereinafter TC) or TrueCopy Extended Distance (hereinafter TCE) configuration via a 10Gbps iSCSI interface.	[Phenomena] A controller failure may repeatedly occur on local side array in TrueCopy remote replication (hereinafter TC) or TrueCopy Extended Distance (hereinafter TCE) configuration via a 10Gbps iSCSI interface. <Web Message> HD2100 Host transfer DMA error was over the threshold(CTL-x,DMA-yz) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.3/A (08B3/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) 10Gbps iSCSI interface is installed. (2) TC or TCE is enabled. (3) Remote path is set via a port of (1). (4) The completion of initiator command of TC or TCE from iSCSI protocol chip firmware is reported in the array on local side. (5) The reception of Ack packet delays due to network pathway failure and retransmission of TCP packet occurs after the condition of (4). [Probability of failure] Medium <Explanation> [Cause] Firmware bug When iSCSI protocol chip firmware receives SCSI response while there is(are) unreceived Ack packet(s) due to a network pathway failure at initiator operation, it may report the command completion to firmware of array system without waiting for the receipt of Ack packet due to the iSCSI protocol chip firmware bug. After this, when iSCSI protocol chip firmware retransmits TCP packet for the command reported the completion based on Ack packet timeout, the firmware of array system detects the status abnormality of command and the controller failure occurs. <Countermeasure> The modification was made on iSCSI protocol chip firmware in order that the firmware of array system will be reported its command completion upon receipt of all Ack packets at initiator operation. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform the following procedures. (1) Dummy-replace the blockaded controller. (2) Remove the failure of network pathway. <Web Message> HD2100 Host transfer DMA error was over the threshold(CTL-x,DMA-yz)	
	V11.7/F, 08B7/F							5/23/2012　407　None
V11.7/F 08B7/F Base System V11.7/E 08B7/E	1	C	A	SD4487174	VB7-0105	System down caused by firmware update to 08B7/D or 08B7/E	When the firmware is updated to 08B7/D or 08B7/E, the system goes down during the firmware updating or controller 0 fails after the firmware updating. <Web Message> - System down case I6HA01 Online microprogram update is started(CTL-1) I6HE01 Online microprogram update will be executed(CTL-1) I42000 Online micro-update(CTL-0) I6HA00 Online microprogram update is started(CTL-0) *A message will not be displayed indicating controller 0 failure. - Controller 0 blockade case W01400 CTL alarm(CTL-0) <Equipment model / Firmware version> DF800H, V11.7/D (08B7/D) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) DF800H (2) Firmware Rev. 08B7/D or 08B7/E (3) I/O commands queued to Port 0A are more than 45 (4) I/O to Port 0A includes Read/Write commands with transfer length of more than 576KB. [Probability of failure]	

							[Cause] When an access violation occurs to mate normal controller due to hardware failure of the other controller, there is a possibility that the array system goes down with both controllers being blocked. Therefore the firmware ver. 08B7/D was improved so as to avoid array system down by detecting a hardware failure at early stage by performing the access violation diagnosis periodically. During the above diagnosis, the firmware newly reserves the local memory and accessed this area periodically. However, there is a bug in reservation process of local memory area which illegally reserves the area redundantly. Therefore, when the memory area is updated by another process, the access violation diagnosis wrongly detects the failure, causing the controller to fail. <Countermeasure> The firmware modified it to reserve local memory area correctly. [Recovery] Apply the fixed firmware. <Action in the case of the failure> In order to avoid the recurrence of a phenomenon, stop the host access first and then do the following procedure. - System down case (1) Reboot the array system. (2) Update the firmware to the fixed firmware or downgrade the firmware to the previous level firmware 08B7/B or prior until a fix			
	V11.7/G, 08B7/G							5/31/2012	413	029
V11.7/G 08B7/G Base System V11.7/F 08B7/F	1	I	-	SD4325062	VB8-0098	Improvement of monitoring timer to detect other controller failure	The improvement was made for other normal controller to detect the failure faster by shortening the time for timer monitoring in order to detect abnormality of controller when monitoring of controller is suspended incorrectly for a long time.			
	2	I	-	SD4450934	VB8-0101	Improvement of firmware update function during downgrade check is unchecked	As for Firmware update installation from Hitachi Storage Navigator Modular 2 CLI, the guard was enhanced so as not to install different types of firmware under the condition of downgrade check being unchecked.			
	3	I	-	-	VB8-0102	Improvement for trap of SNMP	Previously, the failed Trap of SNMP was issued from the port of controller which detected the failure. However, when port was not done the Link UP at the time of Trap issuance, the designation of issuing Trap from the other port of controller was added.			
	4	I	-	-	VB8-0091	Improvement of user interface for iSCSI Digest parameter	The iSCSI Digest setting must be enabled as default from the Data Security view point, and must be able to be disabled to avoid the performance issue or pass Certification Test by user interface using Storage Navigator Modular 2 Ver. 11.75.			
	5	C	A	SD4406976	VB8-0097	Access lost, non-response of array system, controller blockade, or system down occurs due to HSNM2 manipulation.	[Phenomena] The following phenomenon occurs triggered by HSNM2 manipulation(specific details are described in <3>). (1) Non-response on the host, HSNM2, or RAID Manager. (2) When iSCSI I/F is installed, any one of the following phenomena may occur after (1) occurs. (2-1) Controller is blockaded on one side and non-blockaded controller restarts its response. (2-2) Controller is blockaded on one side and non-blockaded controller remains as non-response. (2-3) System down occurs due to the blockade of both controllers. <Web Message> When phenomenon of (2) is occurring. HH7ED4 Microprogram error[ILM] <Equipment model / Firmware version> DF800H, V8.0/A (0880/A) and later DF800EH, V9.0/A (0890/A) and later [Conditions of Occurrence] <Condition 1-1> The phenomenon (1) may occur when all of the following conditions are met. (1) DF800H or DF800EH (2) Copy-on-write SnapShot(SS) or TrueCopy Extended Distance(TCE) is enabled. (3) Any one of the following pairs exists. -TCE pair under the status of PAIR(Paired),			

							[Cause] Firmware bug There was a bug in the exclusive logic of processing for internal operation in array system. The processing of <3> <Operation or the status of array system which may be Conditions of Occurrence> starts its operation after having completed all other processing. At the same time, the start of new processing is deterred, however the start of other processing across the board was incorrectly deterred. Due to this bug, other processing A (The cache releasing process) is started and when the processing B (executed if <Condition 1-1> or <Condition 1-2> is met) waiting for the completion of that ongoing processing is in operation, processing B cannot complete the operation since the start of other processing A is deterred. As a result, dead lock occurs and the array system will not respond. In case that iSCSI is in use, controller may be blockaded due to the dead lock and becomes timeout by processing. Depending on conditions, both controllers are blockaded and system goes down. <Countermeasure> The modification is made in order to avoid dead lock by setting the conditions on start deterrence. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform the following procedures.
	6	C	A	SD3953704	VB8-0099	Countermeasure for incorrectness of normal controller blockade after controller is blockaded due to LSI hardware failure for data transfer.	[Phenomena] When controller is blockaded due to hardware failure of LSI for data transfer, normal controller is incorrectly blockaded and array system may go down. <Web Message> H06D0x [DCTL]The PCI root complex error was detected [E_IRQ6](CTL-x) <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) The controller failure occurs due to hardware failure of LSI for data transfer. (2) Under the condition that the normal controller is excluding an access from the other controller during processing the controller failure of (1), cache read is performed to the other controller which is processing the blockade. [Probability of failure] Low <Explanation> The probability of occurrence of hardware failure (1) is low. Even [Cause] Firmware bug When cache read is performed under the condition that normal controller excludes an access from the other controller to the cache of controller performing controller blockade processing due to hardware failure of LSI for data transfer, it does not recognize the condition of other controller blockade and may incorrectly read incorrect value(0xFF). The array system went down because the normal controller ended up at incorrect blockade due to the continuation of processing by using this incorrect value. <Countermeasure> When normal controller performs cache read from the other controller under the condition that the access from the other controller is being excluded and when "0xFF" is read, it checks whether the other controller performed cache read is blockaded or not. If the controller was blockaded, it was made not to use incorrect value. [Recovery] Apply the fixed firmware. <Action in the case of the failure> (1) Turn OFF the power at the front side of array system. (2) If the power does not turn off, unplug the cable at the rear side of array system. (3) Replace the blockaded controller due to the hardware failure of LSI for data transfer.

	7	C	A	-	VB8-0104	When failure on one side of controller is detected during hardware diagnosis at the start of array system, the array system does not start.	[Phenomena] When failure on one side of controller is detected during hardware diagnosis at the start of array system, a normal controller also fails to boot and array system may not be able to boot. <Web Message> 01424402 MDMA transfer data compare error <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) A specific hardware failure is detected on the controller on hardware diagnosis at the start of array system. [Probability of failure] Low <Explanation> The probability of occurrence is low because a specific hardware failure occurs in low probability at the start of array system. [Cause] Firmware bug In processing at the start of array system, hardware check is performed to detect hardware failure in advance. When a specific hardware failure is detected at this time, a normal controller refers incorrect information of the controller detecting failure and continues to process the start of array system, the processing of the start of array system has failed. <Countermeasure> The modification was made so that, when the specific failure is detected by hardware diagnosis, the blockade processing is correctly performed and the normal controller does not refer the incorrect value of failed controller. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Replace a controller detected the hardware failure. <Web Message> 01424402 MDMA transfer data compare error
	8	C	A	-	VB8-0006	I/O to Guest OS on VMware ESX will fail or LU for Guest OS becomes unrecognized on VMware ESX.	[Phenomena] [Phenomenon A] When two batteries fail at the same time, I/Os to a Guest OS on VMware ESX 5.0 fail. "Valid sense data" will appear in a log for VMware ESX. [Phenomenon B] After Phenomenon A, if you try to reboot the array or ESX during the battery double failure, an LU for the Guest OS becomes unrecognized on VMware ESX. <Web Message> None <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem can occur when all of the following conditions are met. [Phenomenon A] (1) An LU is used for a Guest OS on VMware ESX. (2) The ATS setting is enabled on VMware ESX (VMFS3.HardwareAcceleratedLocking is set to 0) (3) The two batteries fail. (4) I/Os are being performed on the Guest OS. [Phenomenon B] Same for (1) through (4) as Phenomenon A

							[Cause] Firmware bug [Phenomenon A] The original basic policy was that the array does not support the ATS command for the write through mode which is activated by a double battery failure and the array expects the VMware to issue the Reserve/Release command to the array when the array returns an error to VMware. However, contrary to our expectation, the VMware did not issue the Reserve/Release command, so the device exclusion process does not work with the ATS command, which causes I/Os to the Guest OS to fail. [Phenomenon B] The ATS command is issued from the VMware when the VMware ESX is rebooted. Because of this, the device exclusion process does not work with the ATS command so the LU that contains the Guest OS becomes unrecognized. <Countermeasure> The firmware is modified so that during a battery double failure, it accepts the ATS command and performs the write-after operation. [Recovery] Apply the fixed firmware. <Action in the case of the failure> [Phenomenon A] (1) Suspend I/Os. (2) Fix the battery double failure.
	9	C	A	-	VB8-0088	Allocated capacity of Hitachi Dynamic Provisioning(HDP) becomes inconsistent between P-VOL and S-VOL of TrueCopy Extended Distance(TCE) after pair resynchronization or a cycle copy.	[Phenomena] In a configuration where both P-VOL and S-VOL of TCE are virtual LUs, after write and Write Same commands are performed on the P-VOL and then differential data is transferred from the P-VOL to the S-VOL by pair resynchronization or a cycle copy in Paired status, the allocated capacity of HDP becomes inconsistent between the P-VOL and S-VOL. The allocated capacity of the S-VOL becomes larger than that of the P-VOL. <Web Message> None <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.3/A (0893/A) and later [Conditions of Occurrence] The problem can occur when all of the following conditions are met. (1) TCE is enabled. (2) HDP is enabled (3) Both P-VOL and S-VOL are virtual LUs. (4) Write and Write Same commands are performed on a P-VOL. (5) Differential data is transferred from the P-VOL to the S-VOL by pair resynchronization or a cycle copy in Paired status. [Probability of failure] Medium <Explanation> [Cause] Firmware bug The data transfer job checks if the target HDP area can be released with the Write Same command first, and if it determines that the target HDP area can not be released, it transfers the data in that area to the S-VOL. The bug is that the data transfer job does not check if the target HDP area can be released or not before attempting to transfer the data. Because of this, even if another job that is running at the same time releases HDP area with the Write Same command which makes the equivalent area on the S-VOL released, the job incorrectly transfers the data in the area that has been released by the job running at the same time to the S-VOL. As a result, the allocated HDP capacity becomes larger than that of the P-VOL by the capacity that is incorrectly transferred by the job. <Countermeasure> The firmware is modified so that the data transfer job at first checks if the target HDP are can be released after transferring the data in the previous area, and it transfers the data to the S-VOL only when it determines the target HDP area can not be released. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform DP optimization with the zero page reclaiming option to the S-VOL.

	10	C	A	-	VB8-0103 (Same as DF850 V17-0125)	The local array system goes down by pair splitting instruction with CTG unit when TrueCopy remote replication(hereinafter TC) is used.	[Phenomena] When pair split is instructed by CTG unit with TC, both side of controllers are blockaded on local array and system down occurs. If reboot is performed under such conditions, system down occurs and it fails to reboot. <Web Message> HF1C00 Data transfer check error was detected[PAIRERR](CTL-0) HF1C01 Data transfer check error was detected[PAIRERR](CTL-1) <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) TC is enabled. (2) CTG to which more than two pairs belong exists. (3) There exists the pair which fulfills all of the following conditions in CTG of (2). -An internal LU number of P-VOL is the smallest in CTG of (2). -The pair status is PSUE(Failure). (4) There exists more than one pair which fulfills all of the following conditions in CTG of (2). [Cause] Firmware bug When pair split is performed with CTG unit by TC, clear processing of table for data transfer is implemented by all pairs whose condition change due to split. There was a bug to determine pair that changes to this status. Although it is to be determined by all the pairs, only status change which the smallest pairs are the internal LU number of P-VOL have made it determination. When these pairs status are PSUE, status-changeable pairs are incorrectly determined that pairs do not exist even though there exists the pairs whose status changes and clear processing of table will not be performed. When there are pairs with Copy conditions, it refers uncleared table. At this time, the table is determined its status as incorrect and one controller is blockaded. After that, the processing is taken over to the other controller however the same logic works and controller is blockaded. Both controllers are blockaded and system goes down. Even though reboot is performed, system goes down because the same logic works. <Countermeasure> The modification is made so that the determination of status change is to be implemented for all pairs in CTG. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Remove both remote paths and boot.	
	11	C	A	-	VB8-0106 (Same as DF850 V17-0127)	The array goes down when TC pair becomes Failure(PSUE) and remote paths are deleted.	[Phenomena] The array may go down when TrueCopy(TC) pair becomes Failure(PSUE) and remote paths are deleted. The array goes down after rebooting the array. <Web Message> HJ275N Microprogram error[RVM] HJ2726 Microprogram error[RVM] <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] <Condition 1> The problem may occur when all of the following conditions are met. (1) TC is enabled (2) There are TC pairs that satisfy either of the followings (2-1) Pair status is PAIR(Paired) or COPY(Synchronizing) (2-2) Pair status is PSUS(Split) (3) One or more pairs that satisfies (2-1) or (2-2) goes PSUE(Failure) (4) Delete the remote paths immediately after (3) <Condition 2> The problem may occur when all of the following conditions are met.	

							[Cause] Firmware bug In the process of making TC pair PSUE(Failure), the P-VOL is made PSUE(Failure) and then S-VOL is made PSUE afterwards in background. There was a bug in the process of making S-VOL PSUE(Failure). In the process of making PSUE(Failure), remote paths are checked and if there are no remote paths, the controller is blockaded. However, when Conditions of Occurrence are met, there are cases when there are no remote paths. As a result, a controller goes down and the other controller also goes down when the same process is executed. Also, when the array is rebooted, the same process is run and the array goes down again. <Countermeasure> The firmware is modified so that nothing is done if the remote paths don't exist when TC pair goes PSUE, similarly as when the remote paths are blockaded. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Apply the fixed firmware using web and boot the array. <Web Message> HJ275N Microprogram error[RVM] HJ2726 Microprogram error[RVM]
	12	C	A	-	VB8-0043	Controller is blockaded during online parity recovery and array system goes down afterward.	[Phenomena] Controller is blockaded during online parity recovery and array system may go down after displaying the message below. <Web Message> In case of V11.5/A or before: W0L000 Unreadable PIN detected(Unit-x, HDU-y),W0M000 Unreadable PIN detected(Unit-*, HDU-*) In case of V11.5/A and later: Microprogram error was detected[RCH] <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when the following conditions (1) to (3) are met. (1) Virtual LU or normal LU definition in size of more than 2TB. (2) Online parity recovery is being executed. (3) HDD error is detected when staging from HDD to cache is operated. [Probability of failure] Low <Explanation> The probability of multiple occurrences such as HDD errors is low [Cause] Firmware bug In case of V11.5/A or before: When HDD error is detected while online parity recovery is performed, the area where error occurs are registered as write uncompleted area with extended online parity recovery processing. At this time, as there was a bug in a parameter value to be used for write uncompleted registration processing, normal area may be registered as write uncompleted area. In case of V11.5/A and later: When HDD error is detected while online parity recovery is performed, the area where error occurs are registered as write uncompleted area with extended online parity recovery processing. At this time, as there was a bug in a parameter value to be used for write uncompleted registration processing, that write uncompleted processing fails and controller is blockaded. After that, it becomes the state of "Microprogram error was detected[RCH]" and array system may go down. <Countermeasure> The modification was made so that the parameter using in write uncompleted registration processing becomes a normal value. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Recreate LU after having deleted the LU of online parity recovery after array system starts.

	13	C	A	-	VB8-0083	When the array is rebooted without cache volatilization, both controllers blockade may occur and the array system goes down.	[Phenomena] When the array is rebooted without cache volatilization, both controllers blockade may occur and the array system goes down. <Web Message> HJ01xx Microprogram error[INM] <Equipment model / Firmware version> DF800H/EH, V9.3/A (0893/A) and later [Conditions of Occurrence] The problem occurs certainly when all of the following conditions are met. (1) DF800H or DF800EH (2) The array is rebooted without cache volatilization. (3) Invalid configuration information is read from all the system drives (HDU#0 of Unit#0 to HDU#4) due to drive failures in all the system drives at the time of (2). [Probability of failure] High <Explanation> The problem occurs certainly when all of the above conditions are met. [Cause] Firmware bug When the array is rebooted without cache volatilization, and if the configuration information of all the system drives is invalid, the firmware reboots the array using the configuration information on cache memory. At that time, firmware checks whether the configuration information on cache memory is available or not. But the firmware determines that the configuration information is not available due to the firmware bug. Finally, the array rebooting fails. <Countermeasure> The modification was made so that the firmware correctly checks whether the configuration information is available or not. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Update the fixed firmware in maintenance mode of the array without cache volatilization and reboot the array. <Web Message> HJ01xx Microprogram error[INM]	
	14	C	B	-	VB8-0090	When there are TCE pairs and booting without cache volatilization is executed, PSUE(Failure) occurs.	[Phenomena] When there are TrueCopy Extended Distance(TCE) and booting without cache volatilization is executed, the following phenomena occur. <Phenomenon 1> The pair status of P-VOL changes to PSUE(Failure). If deletion of this pair is executed in the local array, the pair is not deleted. <Phenomenon 2> The pair status of P-VOL changes to PSUE(Failure). If deletion or re-synchronization of this pair is executed in the local or remote array, the controller is blockaded in the remote array. <Phenomenon 3> The pair status of P-VOL changes to PSUE(Failure). In this case, re-synchronization or deletion of TCE pair is available. <Phenomenon 3-1> The pair status of P-VOL changes to PSUE(Failure). If there is SS pair with cascading TCE S-VOL, SS pair status changes to PSUE(Failure). In this case, re-synchronization or deletion of TCE pair is available. <Web Message> Phenomena 2: HJ2CRG Microprogram error[POM]	

							[Cause] Firmware bug When rebooting is executed after boot without cache volatilization occurs, the logic to recover incorrect management information operates due to interrupted processing. There was a firmware bug in this recovery logic. Immediately after rebooting, information of temporal memory becomes ALL0 so recovery logic should be implemented after copying management information from non-volatilization memory. However, the recovery logic that operates on condition of <3>Conditions of Occurrence included the management information which is operated before copying. Because of this, recovery logic is implemented with ALL0 information and internal information of S-VOL becomes incorrect status. P-VOL side detects incorrectness of S-VOL side and it changes to PSUE. <Countermeasure> Recovery processing is implemented after management information copy from non-volatilization memory is done at the time of rebooting after boot without cache volatilization occurs. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Phenomena 1: Delete pair in local array after pair deletion in remote array. Re-create pair.
	15	C	B	-	VB8-0082	A planned shutdown does not complete during use of Copy-on-write SnapShot(SS) or TrueCopy Extended Distance(TCE).	[Phenomena] When you execute a planned shutdown to an array that has SS or TCE pairs, it does not complete normally. The array does not accept any operations from HSNM2 or I/Os from the host during that time. <Web Message> None <Equipment model / Firmware version> DF800H, V4.0/A (0840/A) and later DF800EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem can occur when all of the following conditions are met. (1) SS or TCE is enabled. (2) SS or TCE pairs retain replication data (differential data). In other word, write operations have been performed on SS or TCE pairs. (3) Perform a planned shutdown or quasi planned shutdown. [Probability of failure] Low [Cause] Firmware bug On a request for a planned shutdown, jobs start writing dirty data to the drives so the planned shutdown can finish. Those kind of jobs are activated on both cores after the CTLs are confirmed to be synchronized between each other. However, the Y core incorrectly activates the jobs before it is confirmed the CTLs have been synchronized, so the jobs do not complete their tasks normally, which keeps the planned shutdown to complete. Because the array does not accept accesses from HSNM2 or host while performing a planned shutdown, any operations from HSNM2 or accesses from the host can not be executed. <Countermeasure> The firmware is modified so on a request for a planned shutdown, both cores activate the jobs after it is confirmed the CTLs have been synchronized. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform a reboot without cache volatilization. <Web Message>

	16	C	B	-	VB8-0087	The controller blockaded occurs using SI-SS cascading	[Phenomena] The controller blockaded occurs when use the ShadowImage(SI)-SnapShot(SS) cascading pair. <Web Message> HJ11D0 Microprogram error[RCH] <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.0/A (08B0/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) SI and SS are enabled (2) All of the following conditions are met - cascading pair (SI S-VOL/SS P-VOL) - The S-VOL of SI belongs the RAID Group of RAID0 - SS pair status is PSUS(Split) - SI pair status is COPY(Synchronizing) or PSUS(SP)(Split Pending) [Probability of failure] Low <Explanation> Phenomena occurs when all of the following internal conditions are met. [Cause] Firmware bug The write-protected cache data may appears for a few micro seconds under heavy load or failure. In the case of executing differential copying SI pair to SS pair, however, there is not logic for the write-protected cache data. As a result, the write-protected cache data is regarded as illegal data incorrectly and controller is blockaded. <Countermeasure> Add the logic for the write-protected cache data on differential copying SI pair to SS pair. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Recover blockaded controller using dummy replace <Web Message>
	17	C	B	-	VB8-0057 (same as DF850 V16-0032)	Write Time-out of TC pair and remote path failure occur	[Phenomena] The controller is blockaded when execute initial copying or re-synchronization of TrueCopy Remote Replication(TC). And host time-out occurs and replies 0B/C000 to host. <Web Message> W0K0XY Path alarm(Remote-XXXXXXXX,Path-Y) "XXXXXXXX" is array ID "Y" is the number of Port <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) TC is enabled. (2) The P-VOL or S-VOL belongs the RAID Group of RAID5 or RAID6 (3) The pair (2) meets one of the following conditions. - Pair status is PAIR(Paired) and execute host write access to P-VOL - Pair status is COPY(Synchronizing) [Probability of failure] Low

							[Cause] Firmware bug When there is cache data before writing, the cache data writing process are executed periodically. In the case of RAID Group of RAID5 or RAID6, parity data creation is executed up to 16 times until the cache data writing process. There is the firmware bug in executing up to 16 parity data creation. The delay may occurs until parity data creation in the case of drive failure or heavy load. But parity creation repeats uniformly up to 16 times, although delay has occurred. As a result, the influence of delay accumulates and write command timing out of TC pair, remote path failure, and host access error occur. <Countermeasure> Parity creation is interrupted when delay becomes 9 seconds. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Execute pair re-creation or re-synchronization after path recovery using Web or HSNM2. <Web Message> W0K0XY Path alarm(Remote-XXXXXXXX,Path-Y) "XXXXXXXX" is array ID "Y" is the number of Port
	18	C	B	-	VB8-0086	A Controller blockade after SnapShot V-Vol deletes	[Phenomena] After WriteSame command was executed during a DP pool format, Controller blockade after SS-VVOL deletes <Web Message> HJ2Fxx Microprogram error[QFM] <Equipment model / Firmware version> DF800S/M/H, V7.0/A (0870/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] Conditions from (1) to (4) are met in turn, and the problem may occurred when (5) is met. (1)Dynamic Provisioning is enable and Snap Shot,TCE,TC or ShadowImage is Enable. (2)A DP pool format is completed (a chunk format does not work). (3)Page formatting. - WRITESAME command executing. - DP Optimize executing. - When a page of source volume is not assigned and a page of destination volume is assigned,Pair Create,Resync and Restore is executed.(Without SnapShot) (4)Chunk formatting. - Pair split of SnapShot or TCE.Pair is PSUE. Resync of SnapShot. - DP Optimize executing. - Detected illegal Chunk with garbage collection. - When detected cache uncollectable in virtual LU to belong to a [Cause] Firmware bug When firmware carries out a chunk format job, to carry out a job more than a maximum number by mistake when other jobs work. <Countermeasure> When firmware carries out a chunk format job, to carry out a job that other jobs work and do not exceed a maximum number either. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform dummy replacement the blockaded controller. <Web Message> HJ2Fxx Microprogram error[QFM]

	19	C	B	-	VB8-0089	HDD is blockaded by drive command timeout.	[Phenomena] There is a probability that HDD is blockaded incorrectly by command timeout because of IO response delay. <Web Message> I5HZ00 HDU failure is detected[Command retry failed by PDEV time-out of HDU](Unit-XX,HDU-YY) <Equipment model / Firmware version> DF800H/EH, V11.5/A (08B5/A) and later [Conditions of Occurrence] The problem occurs when (1) condition is met and any of (2) or (3) occurs. (1) DF800H, DF800EH. (2) IO load about a HDD for one core is extremely heavier than another core on the same controller. (3) The amount of IO tag number about two cores for a HDD is very high. The IO tag number is over limitation per a HDD. [Probability of failure] Low <Explanation> According to conditions of occurrence <3>, IO command issuance is inhibited by IO tag number limitation. Although tag number in issuance is decreased and IO can be issued, there is a case that PDEV timeout which is monitoring from the timing of IO issuance [Cause] Firmware bug There is a limitation in the number of IO tag that can be issued to HDD at the same time, and the firmware waits for the command issue once when the limitation is exceeded. When command issue waiting was released by decreasing the number of issued IO tags, HDD is blockaded including sinking of specific IO because there is a problem in the method of selecting the issue command. There is a problem of following (1) and (2). (1)A core that works in high IO load can issue the next command immediately after one IO completion, when the number of IO tags is near a limitation and the IO load of both cores is unbalanced. Therefore, the core that works low IO load meets limitation of the number of tag, and IO might sink because the command can not be issued frequently. (2)The limit judgement about the number of tags for a HDD is executed by the total number in both cores. The limit judgment for the second command is executed immediately after judging for the first command in the core. If a limitation of the number of the tags is solved at the time of the limit judgment of the second command, the second command is issued earlier than the first command. So there is a case that the first command may sink. <Countermeasure> (1) For avoiding sinking commands, when a core meets a limitation of the number of the tags and the number of issued IO tags of the own core is higher than another core, the issue of the command in the own core is temporarily inhibited. In this way,	
	20	C	B	-	VB7-0017	When TrueCopy remote replication(TC) or TrueCopy Extended Distance(TCE) is used, a controller blockade occurs with the web message "Microprogram error [LSM]".	[Phenomena] In some cases, a controller blockade occurs in disk array system at a local side of TC or TCE with fibre channel interface. <Web Message> HJ091D Microprogram error[LSM] <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Fibre Channel interface is installed. (2) TC or TCE is enabled. (3) Remote paths are configured with fibre channel interface. (4) There are two or more replication pairs of TC or TCE. (5) LU ownerships of the local LU in pairs explained at (4) are split at distinct cores(in DF800M/S/EM/ES, distinct controllers). (6) Link down/up occurs (e.g. by disconnection/reconnection the cable) at fibre channel port of the local side diskarray configured with the remote path. [Probability of failure] Low <Explanation>	

							[Cause] Firmware bug When link down/up occurred at fibre channel port, the management core of the port starts PLOGI process. When a fibre channel port received LOGO ACC frame, the owner core of the local LU issues a request of PLOGI process to the management core of the fibre channel port. These two types of PLOGI processing occurred at a same time, controller blockade occurs because diskarray attempts double PLOGI processing. <Countermeasure> The modification was made on firmware to process as follow. If a fibre channel port has been processing PLOGI when the fibre channel port receives LOGO ACC frame, the management core of the port doesn't process secondary PLOGI. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy-replace the blockaded controller. <Web Message> HJ091D Microprogram error[LSM]	
	21	C	B	-	VB8-0040	When 10Gbps iSCSI interface is installed, the ready side controller is blockaded and system is down during online firmware update.	[Phenomena] During online firmware update, the ready side controller is blockaded with web message "Microprogram error [ILM]" and system is down. <Web Message> HH7ED4 Microprogram error [ILM] <Equipment model / Firmware version> DF800H/EH, V11.5/A (08B5/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Disk array with multiple core, that is DF800H or DF850EH. (2) 10Gbps iSCSI interface is installed. (3) Perform a online firmware update during SCSI command IO processing. [Probability of failure] Medium <Explanation> The phenomena occurs when two cores in ready side controller issue requests that perform soft reset a 10Gbps iSCSI port to recover ASIC error at specified timing during online firmware update. [Cause] Firmware bug Following explanation assumes that CTL0 is updating side controller, and CTL1 is ready side controller at online firmware update. Then, the management core of port 0A has been changed from 0X to 1X for performing online firmware update. When ASIC error occurred at port 0A and core 1X (the management core of port 0A) detects it, core 1X executes soft reset the iSCSI protocol chip. When core 1Y (not management core of port 0A) detects the error, it issues a request core 1X to perform soft reset. If core 1X receives a request to soft reset after executing soft reset and before recovering port 0A from reset state, core 1X clears the request to avoid double soft reset. But caused by firmware bug, core 1X also clears the flag indicates port 0A still hasn't been recovered from reset state. As a result, the iSCSI protocol chip related port 0A is kept unavailable, and a command issued to the iSCSI protocol chip falls into timeout and causes "Microprogram error [ILM]". Performing online firmware update is one of conditions of occurrence because core 0X (original management core of port 0A) doesn't clear the flag to recover port 0A. <Countermeasure> The modification was made on firmware to process as follow. Temporary management core during online firmware update also processes same path with original management core to avoid double soft reset.	

	22	C	B	-	VB8-0055	After a configuration of 10Gbps iSCSI port, port state is kept in "setting".	[Phenomena] When a 10Gbps iSCSI port settings are configured, the port state is kept in "setting". Then, the port settings never be able to be changed. <Web Message> None <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.0/A (08B0/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) 10Gbps iSCSI interface is installed. (2) An error occurs at 10Gbps iSCSI protocol chip. (3) During recover process from condition (2), configuration port settings request is issued to port A or E related the iSCSI protocol chip. [Probability of failure] Low <Explanation> Probability is low because this phenomena is occurred when iSCSI protocol chip error and configuration request take place at same time. [Cause] Firmware bug A 10Gbps iSCSI protocol chip related with 2 ports. Following explanation is wrote about port A and B related IF0 (about IF1, translated to port E and F). Recovery from iSCSI protocol chip error and configuration port settings, both are implemented with performing soft reset iSCSI protocol chip. After performing soft reset iSCSI protocol chip, related ports are initialized and set state "Normal" in order (at first port A, at second port B). When configuration port A request is issued during recovery from error and only port A is initialized, port A and port B are set to "setting" and related iSCSI protocol chip is attempted to be performed soft reset to configuration. However, caused by firmware bug, soft reset to configuration is canceled to avoid performing double soft reset because this timing is judged to be performing soft reset. Finally, port B is initialized and set to "Normal", port A is kept in "Setting". <Countermeasure> The modification was made on firmware to process as follow. When soft reset to configuration is attempted during performing soft reset, perform soft reset again after completion the soft reset to recovery. [Recovery] Apply the fixed firmware.
	23	C	B	-	VB8-0056	A controller is blockaded when configuration 10Gbps iSCSI port MTU.	[Phenomena] When MTU settings of 10Gbps iSCSI port is changed, web message "iSCSI firmware load failed" is displayed and the controller with the iSCSI port is blockaded. <Web Message> HHA1xy iSCSI firmware load failed (CTL-x, I/F-y) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.0/A (08B0/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) 10Gbps iSCSI interface is installed. (2) Configure 10Gbps iSCSI port settings. (3) During processing configuration, renewal WEB information with web browser. [Probability of failure] Low <Explanation>

							[Cause] Firmware bug To configuration port setting including MTU, soft reset 10Gbps iSCSI protocol chip is performed. During soft reset process, copying process is performed that copies firmware of iSCSI protocol chip to protocol chip RAM. The completion of this copying process is monitored for 40ms timeout. If interrupt is occurred during monitoring completion, and 40ms elapse to processing the interrupt event, cause by firmware bug, monitor process finds an unexpected timeout and the controller is blockaded. <Countermeasure> The modification was made on firmware to process as follow. During copying iSCSI protocol chip firmware to chip RAM process performed, block interrupts and process interrupt after completion copying process. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy-replace the blockaded controller. <Web Message> HHA1xy iSCSI firmware load failed (CTL-x, I/F-y)	
	24	C	B	-	VB8-0096	When discovery request is issued to iSCSI port at system with 1024 target configured, a controller is blockaded.	[Phenomena] If over 1024 targets are configured in the system and issuing target discovery requests to ports placed on same interface (e.g. port A/B) at once, following web message displayed and controller blockaded. <Web Message> H90320 Watch-dog time-out <Equipment model / Firmware version> DF800H/EH, V9.3/A (0893/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) DF800H or DF800EH (2) iSCSI interfaces are installed at all interface card slot. (3) Total count of targets configured at each iSCSI port on the system is over 1024. (4) Issuing target discovery requests to ports placed on same interface at once. [Probability of failure] Medium <Explanation> When conditions (1)~(4) are satisfied and discovery request received at port A side of A/B (port E side of E/F) earlier than another side, the phenomena may occur. [Cause] Firmware bug When iSCSI port receive a discovery request, the iSCSI port transmits the list of all iSCSI target to login configured in system to host. DF800 user can configure 255 targets at a iSCSI port, therefore 2040 targets are able to be configured in a system. If an iSCSI port receive a target discovery, processing to transmit the list takes 6.8sec. Two ports place on a same interface continually process to send response to discovery request without pass the kernel, and it takes 6.8sec * 2 that is over 9sec. Then watch-dog time-out occurs. <Countermeasure> The modification was made on firmware to improve process to make response to discovery request to cut down the amount of calculation time. Then, full configuration of targets is supported. [Recovery] Apply the fixed firmware. Save the number of target configuration in iSCSI port under 128. Issue discovery one by one port. <Action in the case of the failure> Dummy-replace the blockaded controller. <Web Message>	

	25	C	B	-	VB8-0095	When an iSNS server connected and iSCSI port receives SCN, controller blockaded with "Microprogram error [ILM]".	[Phenomena] When iSCSI interface is used with an iSNS server and iSCSI port receives SCN frame, following web message is displayed and controller is blockaded. <Web Message> HH7E29 Microprogram error [ILM] <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) iSCSI interface is installed. (2) iSNS server is connected with an iSCSI port. [Probability of failure] Low <Explanation> The phenomena occurs when condition (1)~(2) is satisfied and iSCSI port receives SCN frame that is over 2KByte length from iSNS server. SCN frame is transmitted when state of an iSCSI port connected to iSNS is changed (e.g. cable disconnection). SCN notification style is depend on iSNS server specification. [Cause] Firmware bug A size of buffer for receiving frame from iSNS server is 2KByte. If iSCSI port receives a longer frame than this buffer, caused by firmware bug, buffer overflow is occurred and overwrites next buffer. Each iSCSI port has 528 buffer for these frames. If the overflow is occurred at 528th buffer, it overwrites manage information for a next port. Therefore, manage information becomes illegal value, it causes "Microprogram error [ILM]". <Countermeasure> When iSCSI port receives a longer frame than 2KByte from iSNS server, buffering only head 2KByte. [Recovery] Apply the fixed firmware. or Don't connect to iSNS server. <Action in the case of the failure> Dummy-replace the blockaded controller. <Web Message> HH7E29 Microprogram error [ILM]
	26	C	B	-	VB8-0067 (same as DF850 V16-0210)	When host connector is removed during online firmware update, unexpected ASIC error detected.	[Phenomena] When host connector is removed from 10Gbps iSCSI port during online firmware update is being performed and processing SCSI command IO with iSCSI interface, ASIC detects an PCI address uncontinuous error. If this ASIC error count is over the threshold, controller is blockaded with following web message. <Web Message> HD2100 Host transfer DMA error was over the threshold <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.5/A (08B5/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) 10Gbps iSCSI interface is installed. (2) Perform an online firmware update during processing SCSI command IO with iSCSI interface. (3) Remove a host connector on update side controller during online firmware update. [Probability of failure] Low <Explanation> If above conditions are satisfied, the phenomena probably occurs. However, if PCI address uncontinuous error is detected, the

							[Cause] Firmware bug When host connector is removed during online firmware update, to stop the iSCSI firmware of the connector removed port, soft reset iSCSI protocol chip is performed. Then, ready side controller executes soft reset a iSCSI port placed on update side controller and initializes management information about transmission. Caused by firmware bug, firmware initializes information related an incorrect port that isn't performed soft reset. Therefore, management information about transmission becomes illegal value and performed unexpected transmission it has already started at past. Finally, ASIC detects an unexpected access and notifies PCI address uncontinuous error. <Countermeasure> Fix the initializing range of management information about transmission correct(related with soft reset port). [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy-replace the blockaded controller. <Web Message> HD2100 Host transfer DMA error was over the threshold	
	27	C	C	-	VB7QA001	Vendor ID of SATA HDD is not displayed on "Drive Information" when replacing the offline drive firmware is performed.	[Phenomena] When replacing the offline drive firmware is performed, Vendor ID of SATA HDD is not displayed on the Web screen. <Web Message> Web message is none. Vendor ID of "Drive Information" on the Web screen is not displayed. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.5/N (08B5/N) and later [Conditions of Occurrence] The problem occurs certainly when all of the following conditions are met. (1) SATA HDD is installed in the array. (2) When replacing the offline drive firmware is performed. [Probability of failure] High <Explanation> The problem occurs certainly when <3> condition is met. [Cause] Firmware bug In DF800 and DF850, formats of the Drive-specific information written from the firmware to HDD is different. HDD used with DF850 cannot be used for DF800 according to the difference of formats of the Drive-specific information because the firmware checks formats of the Drive-specific information of HDD, and the HDD firmware exchange fails. Therefore, reading the Drive-specific information was deleted. However, Vendor ID was not displayed because the ID is written in the Drive-specific information. <Countermeasure> When replacing the offline drive firmware is performed, firmware reads the Drive-specific information to display the Vendor ID and skips to check the formats of the Drive-specific information. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Apply the fixed firmware, and execute replacing the offline drive firmware. <Web Message> None	
	V11.7/H, 08B7/H							6/29/2012　419　-

V11.7/H 08B7/H Base System V11.7/G 08B7/G	1	C	A	-	VB8-0109	Pair status may become PSUE at the completion of the copy when TC pair is created, resynced, or swapped.	[Phenomena] While P-VOL of TrueCopy remote replication (TC) is being write accessed or used by VMWare, if the TC pair or another TC pair is created, resynced, swapped, or deleted, the TC pair or another TC pair that was in COPY status may become PSUE at the completion of the copy. <Web Message> IB1T00 PSUE occurred[TrueCopy](LU-XXXXP/YYYYS) XXXX: LU number of P-VOL YYYY: LU number of S-VOL <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] <Condition 1> The problem may occur when all of the following conditions are met. (1) TC is enabled. (2) There is a TC pair that meets one of the following conditions. (2-1) Pair status is PSUS (Split) (2-2) Pair status is PSUS (Split) or SSWS (Takeover). (3) P-VOL of (2) is being used by VMWare. (WriteSame, XCOPY, ATS, or UNMAP command is issued.) (4) One of the following is instructed. (4-1) Resync the pair of (2-1) [Cause] Firmware bug When TC copy (A) is started, the firmware bug causes incorrect initialize of copied address of another TC copy (B) instead of copied address of TC copy (A). (Regardless of whether TC copy (B) exists or not.) Copied address is promptly updated to the correct value as copy operation progresses, but if write command is received while copied address is incorrect, TC copy operation incorrectly sets the differential bit to ON, possibly causing write data not to be transferred to the array on the remote side. This causes TC pair status to become PSUE at the completion of TC copy. <Countermeasure> The firmware is fixed to make it initialize copied address correctly when TC copy is started. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Resync the TC pair that became PSUE. <Web Message> IB1T00 PSUE occurred[TrueCopy](LU-XXXXP/YYYYS) XXXX: LU number of P-VOL	
	2	C	A	EUC1628707	VB8-0112	Controller blockade may occur during sequential Read host access to DP-VOL.	[Phenomena] Controller blockade may occur when the tuning parameter [Prefetch Next] is disabled (Default: Enabled) and sequential Read host access is being performed to DP-VOL. Array system down occurs if the same phenomena occur on then other controller after one controller was blockaded. <Web Message> One of the following messages is displayed. HJ11xx Microprogram error[RCH] HJ13xx Microprogram error[DSC] H4001x DMA error was detected <Equipment model / Firmware version> DF800S/M/H, V7.0/A (0870/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Dynamic Provisioning is enabled. (2) RAID5 or RAID6 (3) The number of data disks that party group comprises is other than 2D, 4D, 8D, or 16D. (4) The tuning parameter [Prefetch Next] is disabled. (Default: Enabled) GUI path of Hitachi Storage Navigator Modular 2: [Performance]-[Tuning Parameters]-[Multi Stream]-[Prefetch Next] (5) Sequential Read access is performed to DP-VOL.	

							[Cause] Firmware bug When sequential Read host access to DP-VOL is received, the firmware bug in calculating stripe for Read with [Prefetch Next] disabled attempts to transfer the incorrect range of data, resulting in possible controller blockade. (Data remains correct because the error is detected before the data is transferred to the host.) Array system down occurs if the same phenomenon occurs at the other controller after one controller was blockaded. <Countermeasure> The firmware is fixed to make it calculate correctly stripe for Read. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy-replace the blockaded controller. <Web Message> One of the following messages is displayed. HJ11xx Microprogram error[RCH] HJ13xx Microprogram error[DSC] H4091 DMA system error detected	
	3	C	A	-	VB8-0113	Array system down may occur when Forced Parity Correction is performed to DP-VOL.	[Phenomena] Array system down occurs when Forced Parity Correction is performed to DP-VOL where incomplete writing data (*1) is detected. (*1) incomplete writing data: data that became unable to be read due to the multiple HDD failure. <Web Message> When incomplete writing data is detected, one of the following messages is displayed. W0L000 Unreadable PIN detected (Unit-x, HDU-y) W0M000 Unreadable PIN detected (Unit-*, HDU-*) At array system down (both controllers blockade): HJ11xx Microprogram error[RCH] <Equipment model / Firmware version> DF800S/M/H, V7.0/A (0870/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem occurs certainly when all of the following conditions are met. (1) Dynamic Provisioning is enabled. (2) Cache Partition Manager is enabled. (3) RAID6 (4) The number of data disks that parity group comprises is 17D or more. (5) Stripe size is 256 MB. (Default: 256 MB) [Cause] Firmware bug At initiating Forced Parity Correction, if incomplete writing data exits in correction target DP-VOL, the firmware bug in calculating stripe causes incorrect area to be accessed as detection area of Forced Parity Correction, resulting in controller blockade. After that, the other controller continues the operation handed by the blockaded controller, repeating this phenomenon that leads to array system down. <Countermeasure> The firmware is fixed to make it correctly calculate stripe when incomplete writing data is detected. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Do the following. (1) Install the fixed firmware in maintenance mode, and then reboot the array. (2) Recover the incomplete writing data. <Web Message> One of the following Web Messages is displayed when incomplete writing data is detected. W0L000 Unreadable PIN detected (Unit-x, HDU-y) W0M000 Unreadable PIN detected (Unit-*, HDU-*)	

	4	C	B	SD4527276	VB8-0108(1)	Controller blockade may occur repeatedly when NIC Teaming is enabled with iSCSI configuration.	[Phenomena] Controller blockade may occur repeatedly when NIC Teaming is enabled with iSCSI configuration. <Web Message> HD21xy Host transfer DMA error was over the threshold(CTL-x,DMA-y) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.3/A (08B3/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) 10Gbps iSCSI I/F is installed. (2) NIC is used on the host. (3) NIC Teaming is enabled. [Probability of failure] Low <Explanation> Its occurrence depends on packet splitting in the connected Switch and the timing of internal buffer use (iSCSI protocol Chip) at receiving ANS Probe packet. [Cause] 10Gbps iSCSI firmware bug When NIC Teaming is enabled, NIC sends ANS Probe (Ether Type: 0x886D) packet. The 10Gbps iSCSI firmware bug in determining packet may cause the NIC packet to be incorrectly recognized as IPv6 packet. When this happens, the operation of processing IPv6 uses incorrectly internal buffer (iSCSI protocol Chip) to transfer incorrect EDC data. This causes EDC error to occur repeatedly to exceed the DMA error count threshold, resulting in controller blockade. <Countermeasure> The 10Gbps iSCSI firmware is fixed to make it recognize ANS Probe packet as NIC packet correctly. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy-replace the blockaded controller.
	5	C	B	SD4529099	VB8-0108(2)	Host connection may fail due to the Discovery fail with 10GBps iSCSI configuration.	[Phenomena] Host connection may fail due to the Discovery fail with 10GBps iSCSI configuration. <Web Message> None <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.3/A (08B3/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) 10Gbps iSCSI I/F is installed. (2) TCP connection fails to be established due to the network failure. (3) The failure of (2) repeats 256 times. [Probability of failure] Low <Explanation> [Cause] 10Gbps iSCSI firmware bug When TCP connection establishment fails by receiving TCP-RST or FIN from host or not responding to ACK at network failure during TCP connection establishment (TCP-SYN sequence), internal resources remain incorrectly due to the 10Gbps iSCSI firmware bug in clear operation of internal buffer (iSCSI protocol Chip). When this repeats 256 times, internal buffer is depleted, resulting in not responding to TCP-SYN. This prevents Discovery from being done and host connection from being established. <Countermeasure> The 10Gbps iSCSI Firmware is fixed to make it clear the internal buffer when TCP connection fails to be established. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Planned shutdown and reboot the array. <Web Message> None

	6	C	B	-	VB8-0107	Command response may be delayed at unresponsive HDD failure.	[Phenomena] Command response may be delayed at unresponsive HDD failure. <Web Message> I5HZ00 HDU failure is detected[Command retry failed by PDEV time-out of HDU](Unit-XX,HDU-YY) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.0/H (0890/H) and later [Conditions of Occurrence] The problem may occur when the following condition is met. (1) HDD has permanent unresponsive failure. [Probability of failure] Medium <Explanation> Its occurrence depends on R/W command issue timing when permanent unresponsive HDD failure occurs. [Cause] Firmware bug When HDD R/W command times out, reset command is issued to HDD to reset R/W command. When HDD has permanent unresponsive failure, HDD is blockaded earlier as timeout count of reset command exceeds its threshold. However, the firmware bug in HDD blockade operation prevents HDD from being blockaded as timeout count of reset command exceeds its threshold. After that, HDD is blockaded as failsafe command timeout exceeds its threshold, but this is delayed. Host command response is also delayed because R/W command before blockade is processed after HDD blockade. <Countermeasure> The firmware is fixed to make it blockade HDD when reset command timeout exceeds its threshold. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Replace the blockaded HDD. <Web Message> I5HZ00 HDU failure is detected[Command retry failed by PDEV time-out of HDU](Unit-XX,HDU-YY)
	7	C	B	-	VB8-0111	Controller blockade may occur if a failure occurs at three HDDs in RAID6.	[Phenomena] Controller blockade may occur if a failure occurs at three HDDs in RAID6 and verify error is detected by online verify operation due to the HDD failure. <Web Message> H20100 Parity generation LA error[DRR] <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) RAID6 (2) A failure occurs at three HDDs of (1). (3) Verify error is detected by online verify error function due to the HDD failure of (2). (4) The same controller (*1) detects the error of (3) and has ownership for the LU where the error of (3) was detected. *1: Controller varies depending on the unit number. (Even: CTL-0, Odd: CTL-1) [Probability of failure] Low

							[Cause] Firmware bug In online verify operation, Read for correction is performed to another HDD to perform data check to next block of the error block when verify error is detected. However, if Read for correction fails due to the two HDD errors, the firmware bug in determining ability of correction causes correction to be performed incorrectly. The resulting inconsistent correction data leads to controller blockade. Verify error at one HDD and Read for correction errors at other two HDDs cause the problem. <Countermeasure> The firmware is fixed to make it refrain from performing correction if Read for correction fails. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Do the following. (1) Replace HDD in failure. (2) Dummy-replace the blockaded controller. <Web Message> H20100 Parity generation LA error [DRR]		

	8	C	B	-	VB8-0110 (Same as DF850 V20-B010)	Host error log may be recorded or controller blockade at array on local side may occur in TC or TCE configuration connected with iSCSI I/F.	[Phenomena]
							In TrueCopy remote replication (TC) or TrueCopy Extended Distance (TCE) configuration connected with iSCSI I/F, the following phenomena may occur.
							Phenomenon 1: Host error log is recorded due to disconnection and reconnection of TCP connection during host I/O.
							Phenomenon 2: Controller blockade occurs at array on local side.
							
							<Web Message>
							Phenomenon 1: None
							Phenomenon 2: HD21xy Host transfer DMA error was over the threshold(CTL-x,DMA-y)
							
							<Equipment model / Firmware version>
							DF800S/M/H, V4.3/A(0843/A) and later
							DF800ES/EM/EH, V9.0/A (0890/A) and later
							
							[Conditions of Occurrence]
							The problem may occur when all of the following conditions are met.
							(1) iSCSI I/F is installed.
							(2) TC or TCE is enabled.
							(3) At array on remote side of (2), normal LU, LU that is not the pair LU of (2), is created.
							(4) At array on remote side of (2), the same iSCSI Port shares remote path and host access.
							(5) Data transfer timeout occurs due to the network failure.
							
							[Probability of failure]
							[Cause]
							Firmware bug
							At array on remote side connected with iSCSI, the following are done when data transfer timeout is detected.
							To command from host: Abort command operation, and then return Check condition response (sense key/sense code: B/4B00) to the host. (Operation A)
							To command from array on local side: Do nothing. (Operation B)
							
							However, the firmware bug in recognizing the initiator from which the command is issued may cause incorrect recognition of host and array on local side, leading to the following phenomena.
							If (Operation B) is done to host command: Error log is recorded on host due to the command abort timeout leading to disconnection and reconnection of TCP connection. (Phenomenon 1)
							If (Operation A) is done to command from array on local side: Controller blockade occurs due to DMA error caused by receiving unexpected response at array on local side. (Phenomenon 2)
							
							<Countermeasure>
							The firmware is fixed to make it recognize correct command initiator when data transfer timeout is detected.
							
							[Recovery]
							Apply the fixed firmware.
							
							<Action in the case of the failure>
							Do the following.		

	V11.7/K, 08B7/K							8/10/2012	424 031

V11.7/K 08B7/K Base System V11.7/H 08B7/H	1	I	-	-	VB8-0127 (Same as DF850 V20QP012)	Improvement of load balancing feature	Load balancing feature executes the following processing to equalize CPU utilization each cores. "The owner of the LU that CPU utilization is the highest in the high load core is changed to the low load core." As a result of load balancing, the switched core amounts to high load and the performance may be degraded because of changing owner by load balancing again. Now performance deterioration is prevented by changing to the following processing to not repeat the switch of the owner by load balancing. "When the owner of the LU that CPU utilization is the highest in the high load core is changed, the firmware confirms the load status of the switched core and selects the LU of CPU utilization that load does not raise by switching owner so much."	
	2	C	A	EUC1643962, SD4420815, SD4627254	VB8-0134	SAS HDD may be blockaded during online firmware exchange or at HDD media error.	[Phenomena] If SAS HDD is blockaded during online firmware exchange or at HDD media error and multiple HDD failures occur, responding to the host may become impossible for 10 seconds. <Web Message> Normal HDD blockade case IY0000 HDU error report(Unit-x, HDU-y)[02-0401] W09zab HDU alarm (Unit-x, HDU-y, Type-c) Multiple HDD failure case I30100 HDU error (Unit-x, HDU-y) I41700HDU error over (Unit-x, HDU-y)[IFUNR] <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later HDD Products/Version:DF-F800-AKH600/AKH600X/AKH450/AKH450X/AKH300/AKH146, D02A and before [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) HGST SAS HDD is mounted. (Note1) (2) HDD FW is D02A and before (3) Online firmware exchange is performed or HDD media error occurs. [Cause] HDD firmware bug An internal reset may occur in the HDD due to the HDD-FW bug when an HDD operates ATI (Adjacent Track Interference) prevention in Idle state. The HDD continues to report 02/0401 error for around 10 seconds until a reboot process completes. An HDD transits to Idle state when an access to the HDD stops for more than 0.5 second. ATI prevention is performed under specified conditions in the Idle state. The HDD-FW bug may appear in ATI prevention process with specified conditions. The array firmware blockade HDD if 02/0401 (Becoming Ready) is sent during I/O. If internal reboots occur in multiple HDDs in single RAID group, the array firmware cannot respond to the host until internal reboots are finished. <Countermeasure> HDD firmware was fixed to prevent internal reset even if confliction between ATI Prevention and command occurs. [Recovery] Apply the fixed firmware. <Action in the case of the failure> (a) An HDD fails w/o "HDU Error" message. (Normal HDD	

	3	C	A	SD4501956	VB8-0129	Array system down may be caused by ENC blockade during online firmware exchange.	[Phenomena] During online firmware exchange or following automatic ENC firmware exchange in one controller, array system down may be caused by the blockade of the other controller or the backend ENC of it. <Web Message> HH8W00 Backend has been down[All the routes have been blockaded] or HH750x Backend link error was detected(CTL-x) <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later ENC Firmware for RKAKS, 07-02-13 and later ENC Firmware for controller, RKAK, and RKAKX, 06-01-12 and later [Conditions of Occurrence] The problem may occur when the following condition is met. (1) Online firmware exchange is performed. [Probability of failure] Low <Explanation> Its occurrence depends on command operations and ENC command response timing. [Cause] ENC firmware bug While online firmware exchange or following automatic ENC firmware exchange is being performed in one controller; when the other controller is issuing commands to drive and ENC, drive command is given priority due to the incorrect handling of command sequence and response to commands from the array firmware may be neglected. In this case, ENC is blockaded by the array firmware after detecting unresponsive ENC. This blockade is performed by the ENC in the backend of the controller which is not in exchanging operation, resulting in array system down. Controller blockade may occur instead of ENC blockade because DF800S/M/ES/EM controller has ENC. <Countermeasure> Command process sequence of ENC firmware is fixed to process response to the array firmware. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Turn OFF/ON the main switch of the array system, and then apply the fixed firmware. <Web Message> HH8W00 Backend has been down[All the routes have been blockaded]
	4	C	A	SD4684124	VB8-0140	Controller may be blockaded if sequential Read host access is received during DP pool drive recovery.	[Phenomena] Controller may be blockaded if sequential Read host access is received during DP pool drive recovery. <Web Message> HJ11OV Microprogram error[RCH] <Equipment model / Firmware version> DF800S/M/H, V7.0/A (0870/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Dynamic Provisioning is enabled. (2) RAID level is RAID 5 or RAID 6. (3) The number of data disks which Party Group comprises is other than 2D, 4D, 8D, or 16D. (4) Drive recovery (correction copy) is being performed after a failure in the drive which belongs to the DP pool. (5) Sequential Read access to virtual LU is received. [Probability of failure] Medium <Explanation> Its occurrence depends on the access pattern of sequential Read.

							[Cause] Firmware bug When prefetch is performed after receiving sequential Read host access to virtual LU; if DP pool is assigned over pages, incorrect calculation of stripe rows causes incorrect prefetch, resulting in controller blockade. <Countermeasure> The firmware is fixed to correctly calculate stripe rows. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Do the following. (1) Turn OFF the prefetch until the drive recovery is finished. (Set 0 in Count of Judgment Sequential (default: 3) of Tuning Parameters. (HSNM2 GUI path: [Performance]-[Tuning Parameters]-[Multi Stream]-[Edit System Multi Stream]-[Count of Judgment Sequential].) (2) Dummy-replace the blockaded controller. <Web Message> HJ11OV Microprogram error[RCH]	
	5	C	A	-	VB8-0138	Controller blockade may occur during data recovery of a virtual LU.	[Phenomena] Controller blockade may occur during data recovery for a drive of DP pool. <Web Message> HF0106 Data transfer check error[WSEGLOCK] <Equipment model / Firmware version> DF800S/M/H, V7.0/A (0870/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when conditions of both (1) and (2) are met, and then any one of the operations of (3) to (6) is performed. (1) Dynamic Provisioning is enabled. (2) An error occurs in a drive of DP pool and data recovery is in progress. (3) Load balancing function changes LU ownership to other core for the LU in the data recovery because command load is high. (4) Replication feature (Copy-on-write SnapShot, ShadowImage in-system replication, TrueCopy remote replication, TrueCopy Modular Distributed, TrueCopy Extended Distance, Modular Volume Migration) is used and pair is created. (5) LU ownership is changed from HSNM2. (6) Cloning is performed on VMware. [Probability of failure] Medium [Cause] Firmware bug The firmware incorrectly continues the prefech processing without changing the target area due to the bug of reference means of target area when LU ownership is changed during activation of prefech processing in the prefech process running on the core in the data recovery. <Countermeasure> The firmware is fixed the reference of the target area of the prefech processing. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy-replace the blockaded controller. <Web Message> HF0106 Data transfer check error[WSEGLOCK]	

	6	C	A	SD4638646	VB8-0130	Delayed response to the host at SATA HDD failure	[Phenomena] When SATA HDD failure occurs, response to the host I/O to the LU in the faulty HDD may be delayed by about 18 seconds. <Web Message> None <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) SATA HDD is mounted. (2) A specific failure occurs on SATA HDD (3) SATA HDD of (2) receives host I/O. [Probability of failure] Medium <Explanation> The phenomenon occurs when a specific failure (Device Fault) occurs. [Cause] SAS protocol chip firmware bug Even if a failure (Device Fault) is reported from SATA HDD to the SAS protocol chip following the SATA HDD failure, SAS protocol chip does not notify the array firmware of the failure. This causes the array firmware to stop command execution and send data to the host by correction copy after 18 seconds in total (internal timeout (9 seconds) and command retry timeout (9 seconds)). <Countermeasure> SAS protocol chip is fixed to notify the array firmware of failure from SATA HDD (Device Fault). [Recovery] Apply the fixed firmware. <Action in the case of the failure> If SATA HDD is blockaded, replace the blockaded HDD. <Web Message> I5HZ00 HDU failure is detected [Command retry failed by PDEV time-out of HDU] (Unit-x, HDU-y) W09zab HDU alarm (Unit-x, HDU-y, Type-c)
	7	C	A	SD4535389	VB8-0117	Host access response may be delayed during SATA drive recovery.	[Phenomena] Host access response may be delayed during SATA drive recovery. <Web Message> None <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) SATA drives are used for the RAID group of RAID 5 or RAID 6. (2) A drive failure occurs in the RAID group of (1), and then drive recovery (correction copy) is performed. (3) Write access is received to the LU in the RAID group to which correction copy is being performed. (4) Commands such as inquiry and ModeSense are issued from the host periodically for health check. [Probability of failure] Medium <Explanation> The phenomenon occurs if the conditions are met and heavy load is imposed on the core other than the core to which correction copy

							[Cause] Firmware bug Recovery process is performed on a single LU basis by the core which has LU ownership and another core is checking its turn periodically. But the incorrectly short checking interval causes frequent checking operations, resulting in CPU usage rates being higher on the core in recovering than those on the core in waiting. Responding to this, the load balancing assigns too much LU ownership to the core in recovering to delay the response to the prioritized commands such as inquiry and ModeSense, which are issued from the host periodically, resulting in possible delayed responses to the commands such as Read and Write. The checking interval of drive recovery is fixed to prevent causing incorrectly high CPU usage rates. <Countermeasure> The checking interval of drive recovery was fixed to prevent causing incorrectly high CPU usage rates. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Do the following. (1) Disable load balancing during the drive recovery. (Hitachi Storage Navigator Modular 2 GUI Path: [Performance]-[Tuning Parameters]-[System Tuning]-[Edit System Tuning Parameters]-[Load Balancing])
	8	C	A	-	VB8-0126	Failure to respond to host commands at controller blockade	[Phenomena] In DF800H or DF800EH, operating controller may become unresponsive to host commands while the other controller is in blocked state for any reason like hardware failure. <Web Message> None <Equipment model / Firmware version> DF800H, V4.0/A (0840/A) and later DF800EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) DF800H or DF800EH (2) A command (*1) is issued from the other controller(CTL-A) to the LU whose ownership is assigned to the Y core. (3) Before CTL-A transfers the command of (2) to the controller(CTL-B) of Y core which has the ownership, CTL-B is blockaded. (*1) Format Unit(0x04), Mode Select(6)(0x15), Sync Cache(0x35), Mode Select(10)(0x55), Write Buffer(0x3B), Persistent Reserve Out(0x5F), Sync Cache(16)(0x91), LAN Select(0xE0), Write commands from CCI(RAID Manager), and TC/TCE operation commands from HSNM2 or CCI(RAID Manager) [Cause] Firmware bug When CTL-B is blockaded, commands are processed by CTL-A after LU ownership is given instead of transferring commands to CTL-B. But LU ownership change fails because of the incorrect determination process in changing LU ownership, resulting in commands not being processed. <Countermeasure> Determination process in changing LU ownership is fixed. [Recovery] Apply the fixed firmware. <Action in the case of the failure> To discard the command, disconnect, and then connect the cable on the Port on which the unresponsive LU is mapped. <Web Message> None

	9	C	A	-	VB8-0124	Isolation of failure point in backend may become impossible after a temporary hardware failure occurs in the controller.	[Phenomena] After a temporary hardware failure occurs in the controller while ENC, HDD, controller, or ENC firmware is being exchanged; if another failure occurs in any of the ENC, HDD, controller SAS protocol chip, failure point becomes unable to be isolated, resulting in the failure point being unable to be blockaded. If a failure occurs in ENC or controller SAS protocol chip, redundancy of the backend path is lost because the failure point is left as it is. If online firmware exchange is performed after this happens, the firmware exchange fails with the message of "DMES05EA42" in HSNM2. <HSNM2 Error Message> DMES05EA42 The process cannot be performed because the subsystem is under diagnosis process. Please retry after a while. <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) The following part is exchanged and automatic ENC firmware exchange operation is performed following the exchange. - Exchange the ENC, HDD, or controller. Automatic ENC firmware exchange is performed following [Cause] Firmware bug If controller reset is performed due to a temporary hardware failure while ENC, HDD, controller, or ENC firmware is being exchanged, the incorrect initial settings cause the internal state to be "under exchanging process" even after the exchange operation. After that, even if a failure occurs in any of ENC, HDD, or controller SAS protocol chip, the internal state of "under exchanging process" prevents isolation of failure point, resulting in isolation being waited for. If the isolation of failure point is being waited for, online firmware exchange also cannot be started. <Countermeasure> The firmware is fixed to not hold incorrectly the internal state of "under exchanging process". [Recovery] Apply the fixed firmware. <Action in the case of the failure> If online firmware exchange fails with the message of "DMES05EA42", do the following. (1) Retry online firmware exchange in 10 minutes. (2) If a similar message appears again, do planned shutdown. (3) Retry online firmware exchange after the reboot. <HSNM2 Error Message> DMES05EA42 The process cannot be performed because the	
	10	C	B	-	VB8-0119 (Same as DF850 V20-0282)	TrueCopy Extended Distance (TCE) pair status may become Failure by receiving vStorage commands	[Phenomena] Pair status may become Failure when P-VOL receives vStorage commands (Xcopy/Write Same/ATS/Unmap) at creation, resync, or swap of TCE pair. <Web Message> Pair status changed by the error(CTG-X) Remote copy failed(CTG-X) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.3/A (0893/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) TCE is enabled. (2) TCE pair is performed creation, resync, or swap. (3) When (2) is performed, the status becomes one of the following conditions involving copy speed, bandwidth of remote path, and the number of pairs in TCE copy per controller. (3-1) Copy speed: fast or medium Bandwidth: 12.0 to 44.9 Mbps Pairs in TCE copy: 2 or more (3-2) Copy speed fast or medium Bandwidth: 0.2 to 11.9 Mbps Paris in TCE copy: 1 or more (3-3) Copy speed: slow Bandwidth: 3.0 to 5.9 Mbps Pairs in TCE copy: 3 or more	

							[Cause] Firmware bug At creation/resync/swap of a pair, its copy is performed turning differential bits OFF from ON; however, if the same area as the data area for differential bits in copying receives vStorage commands, the firmware bug incorrectly turns ON differential bits. This causes an error to be detected at differential bit check at completion of creation, resync, or swap of the pair, resulting in the pair status becoming Failure. <Countermeasure> The firmware was fixed to avoid incorrectly turning ON differential bits when the same area as the data area for differential bits in copying receives vStorage commands. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Do the following. (1) Disable vStorage commands in the host group option using Hitachi Storage Navigator Modular 2. The following two modes are disabled. Unique Extended COPY mode Unique Write Same mode (2) Resync the TCE pair whose status has become Failure. <Web Message> Pair status changed by the error(CTG-X)
	11	C	C	-	VB8-0128 (Same as DF850 V20QA010)	Load balance between controller and core is not improved by incorrect load balance feature.	[Phenomena] By incorrect load balance feature, CPU utilization becomes high in the switched controller and core after owner switch by load balance. And load balance is not improved, and an owner switch by load balance occurs repeatedly. <Web Message> None <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) The load balance feature is enabled. (2) An array receives I/O that CPU load balance is different between each controller and core. (3) The some LU exists in a controller and core detected to be high load, but the number of LU is a few comparatively. (4) The LU in a controller and core detected to be high load belongs to an each other RAID level. [Probability of failure] Low <Explanation> [Cause] Firmware bug A load balance feature consists of the following three phases processing. Phase 1: A high load controller and core is searched, and a source controller and core which moves LUs is decided. Phase 2: A low load controller and core is searched, and a destination controller and core which moves the LUs is decided. Phase 3: To bring load balance between controller and core close to an equal status, switch target LU is selected, and switched. For Phase 3 processing to select switch target LU, the score each LU is calculated and the CPU utilization each LUs is calculated by that score ratio and the LU to get most load balance is selected. The score is calculated from category-weighting factor considered Hit Read, Miss Read, Write I/O count and RAID level and so on. But category-weighting factor has a bug. Therefore the load balance between controller and core is not improved after LU switch to select the switch target LU by incorrect score. <Countermeasure> This firmware is fixed in the correct number in the category-weighting factor. [Recovery] Apply the fixed firmware. <Action in the case of the failure>

	12	C	C	-	VB8-0125 (Same as DF850 V20-S018)	A progress indication during formatting DP pool is displayed incorrectly.	[Phenomena] The DP pool format progress in the DP RAID group during recovering drive is displayed incorrectly. <Web Message> None <Equipment model / Firmware version> DF800S/M/H, V7.0/A (0870/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Dynamic Provisioning is installed and enabled. (2) DP pool is formatting by the user operation, DP pool creation, DP pool reinitialization, DP pool capacity addition, Virtual LU deletion and Virtual LU format. (3) Execute the drive recovery in the DP pool during formatting. (4) The remaining capacity that should be formatted is less than the capacity of the drive recovery. [Probability of failure] High <Explanation> It occurs when this condition of occurrence are satisfied. [Cause] Firmware bug When the drive recovery and DP pool format is executed at the same time, the progress is calculated incorrectly. Therefore it is shown incorrectly to input an illegal value into a table managed for displaying progress. <Countermeasure> The firmware is fixed by calculating correctly when the drive recovery and DP pool format is executed at the same time. [Recovery] Apply the fixed firmware. <Action in the case of the failure> - Wait for the following web message which is shown when a format is completed. - When the drive recovery is completed and Web messages is not shown, shutdown and start the array. <Web Message> I6HL00 DP pool format completed(DP Pool-XX)	
	13	C	C	-	VB8-0131 (Same as DF850 V20-0137)	A notification is not issued for the part failure and part recovery for intermittent hardware error.	[Phenomena] When a part fails or recovers after failure, the notification of the part failure and part recovery is not issued. <Part failure> (a) The failure messages and failure part position is not shown in the maintenance Web window. (b) The failure notification is not shown in the HSNM2. (c) The E-mail and SNMP notification is not issued. (d) The Warning LED in the front of array and the LED on the failure part and is not lit. <Part recovery> (a) The failure notification is not shown in the HSNM2 and maintenance Web window. (b) The Warning LED in the front of array and the LED on the failure part and is not lit out. <Web Message> None <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence]	

							[Cause] Firmware bug When the intermittent hardware error occurs during the part failure or recovery part, the following notifications are not issued because the table that manages part failure or part recovery is updated incorrectly. <Part failure> (a) The failure messages and failure part position is not shown in the maintenance Web window. (b) The failure notification is not shown in the HSNM2. (c) The E-mail and SNMP notification is not issued. (d) The Warning LED in the front of array and the LED on the failure part and is not lit. <Part recovery> (a) The failure notification is not shown in the HSNM2 and maintenance Web window. (b) The Warning LED in the front of array and the LED on the failure part and is not lit out. <Countermeasure> The firmware is fixed by not updating the table that manages part failure or part recovery incorrectly when the intermittent hardware error occurs. [Recovery] Apply the fixed firmware.		
	V11.7/N, 08B7/N							8/31/2012	426 -
V11.7/N 08B7/N Base System V11.7/K 08B7/K	1	I	-	SD4406440, EUC1640292	VB8-0137(1)	Expansion of the network buffer size	To compete against very frequent security-attacks, the buffer (=work area) of the network function of the array is expanded. Thus the network function will not halt its services and the controller will not fail.		
	2	I	-	SD4406440	VB8-0137(2)	Improvement of the Web server function	When the array receives an illegal access (to non-existing URL) to its Web server, the Web server function of the array waits for 1 second to avoid consuming the CPU time of the array for the illegal access and the retrying accesses. Other functions of the array will work as usual.		
	3	I	-	SD4623854	VB8-0153	Improvement of remote path creation	Remote path may be failed to be created due to the controller reset (CHK1 reset) caused by the inconsistency between the login status and the remote path status at the creation of the remote path. Responding to this, the firmware was fixed to successfully create the remote path by refraining from the reset at the creation of the remote path, checking the login sequence and the internal login status, and retrying the remote path login. In addition, the firmware collects more information about login sequence.		
	4	I	-	-	VB8-0147	Improvement in host I/O performance during dynamic sparing	Improvements are made to switch to correction copy if a response delay is detected by periodically checking response time of the failed HDD in order to prevent degradation of host I/O performance caused by a response delay of the failed HDD during dynamic sparing.		
	5	C	A	SD4656444	VB8-0145	Array system down may occur due to the blockage of both controllers during dynamic sparing of HDD in RAID 6.	[Phenomena] In the RAID group of RAID 6, if unreadable data (unreadable PIN data) exists on two or more HDDs other than the error-ridden HDD, both controllers are blocked, resulting in array system down. <Web Message> If unreadable data (unreadable PIN data) exists: W0L000 Unreadable PIN detected(Unit-x,HDU-y) If controllers are blocked: HZ0N00 Kernel processing error(CTL-0) HZ0N01 Kernel processing error(CTL-1) <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) RAID group is RAID 6. (2) During dynamic sparing of a HDD in (1), many errors occur in the HDD. (3) Data recovery method is switched from dynamic sparing to correction copy due to (2). (4) Unreadable data (unreadable PIN data) in the same LBA is detected on two or more HDDs (other than the HDD that has many		

							[Cause] Firmware bug In dynamic sparing, data is recovered by copying between drives. If many errors occur on the HDD from which data is copied, data recovery method is changed from dynamic sparing to correction copy. After that, if unreadable data (unreadable PIN data) in the same LBA is detected (Failure A), the LBA must be skipped and the next LBA must be recovered. However, the firmware bug fails to skip the LBA only to prevent the operation, resulting in controller blockage. After that, the other controller continues the data recovery only to be blocked, resulting in array system down. <Countermeasure> The firmware is fixed to skip the LBA where Failure A is detected in data recovery by correction copy switched from dynamic sparing and to perform data recovery of the next LBA. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform the following procedure. (1) Turn OFF the main switch, and the turn it ON to boot the array. (2) Click "Manual" in [Drive Restoration]. Drive Restoration: [Settings]-[Drive Recovery]-[Edit Recovery Options]-[Drive Restoration] in Hitachi Storage Navigator Modular 2. (3) Accoring to the message of "W0L000 Unreadable PIN
	6	C	A	-	VB8-0152 (Same as DF850 V20-B036)	When the online firmware update is executed again after the controller failure and recovery during the online firmware update, an array is down.	[Phenomena] For TrueCopy remote replication or TrueCopy Extended Distance, when the online firmware update is executed again after the controller failure and recovery during the online firmware update, an array is down. <Web Message> HH7EEL Microprogram error[ILM] <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. (1) TrueCopy remote replication or TrueCopy Extended Distance is installed. (2) The remote path with iSCSI is connected. (3) The same port is used to connect the remote array and server. Or, it is bi-directional configuration. (4) Execute the online firmware update. (5) The controller 0 is blocked during the online firmware update in the controller 0. (6) Execute the online firmware update after recovery the controller 0 of (5). [Probability of failure] High [Cause] Firmware bug When the controller 0 is executing the online firmware update, the controller 1 executes login processing referring to the iSCSI login management information in the controller 0. This information is specified the target ID for TrueCopy remote replication or TrueCopy Extended Distance or the initiator ID for server connection. Therefore, in referring to this information in iSCSI login, TrueCopy remote replication or TrueCopy Extended Distance and the server connection can be decided. When the controller 0 is blocked during the online firmware update, iSCSI login information in the controller 0 is not cleared incorrectly. The controller 1 refers to the incorrect information before the controller 0 failure and detects the different from the current login information and the login information in the management information and then logic inconsistency occurs. <Countermeasure> The firmware is fixed to clear the login management information in the controller 0 for the recovery processing in the controller 0 failure. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Start the array and execute the firmware update with reboot. <Web Message>

	7	C	A	-	VB8QA007	Array system down may occur when a temporary failure of the 10Gbps iSCSI interface occurs in the controller #0 during online firmware update.	[Phenomena] Array system down may occur when a temporary failure of the 10Gbps iSCSI interface occurs in the controller #0 during online firmware update. <Web Message> HHA1XZ iSCSI firmware load failed(CTL-X,I/F-Z) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.0/A (08B0/A) and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. (1) A 10Gbps iSCSI interface is used. (2) Controller #1 replacement has been performed while the array is online. (3) No planned shutdown has been performed since (2). (4) Online firmware update is performed. (5) Temporary failure of the iSCSI protocol chip in the 10Gbps iSCSI interface occurs during rebooting of firmware update in the controller #0. [Probability of failure] High <Explanation> This problem occurs when all of the conditions are met. [Cause] Firmware bug When a temporary failure of the 10Gbps iSCSI protocol chip (Failure A) occurs during rebooting of the controller #0 at online firmware update, the controller #1 in Ready initializes the chip. Preparing for later initialization, chip initialization information is copied in advance between the controllers when the array is booted or a controller is replaced. However, Bug 1 causes the initialization information to not be copied from the controller #0 in Ready to the replaced controller #1, resulting in initialization failure due to the incorrect initialization information when Failure A occurs. At this time, Bug 2 causes the controller #1 in Ready to be blocked instead of the controller #0 where chip initialization fails, resulting in array system down. <Countermeasure> The firmware is fixed to: (1) Copy the initialization information for the 10Gbps iSCSI protocol chip in the controller in Ready to the replaced controller. (2) Block the correct controller when initialization of the 10Gbps iSCSI protocol chip fails at Failure A. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform the following procedure. (1) Turn OFF the main switch, and then turn it ON to boot the array.
	8	C	A	-	VB8-0146 (Same as DF850 V20-S036)	After swapping and power down with cache volatilization for TrueCopy Extended Distance, a controller is blocked by creating and deleting pairs.	[Phenomena] After swapping pair in the TrueCopy Extended Distance, when the power down with cache volatilization occurs in the array of primary volume before swapping pair, a pair attribute of volume which changed in the secondary volume by swap processing goes back to the primary volume and the pair attribute both volumes in the pair becomes the primary volume. Then the pair deletes in the array which occurs power down with cache volatilization and when the pair with the primary volume as the volume which deleted a pair creates, the both controller are blocked and an array is down. After power cycle the array, an array is down again. <Web Message> HJ271J Microprogram error[RVM] <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) TrueCopy Extended Distance is installed. (2) Swap a pair for TrueCopy Extended Distance. (3) The power down with cache volatilization occurs within five minutes in the array which changes to the secondary volume after swapping pair, in other words, in the array which exists the primary volume before swapping the volume.

							[Cause] Firmware bug Swapping pair, the secondary volume before swapping pair is specified in the internal information. This information is deleted when a pair deletes from an array of the primary volume. Within five minutes after swapping pair, when the power down with cache volatilization with an array of the primary volume before swapping the primary volume occurs, the information that the pair attribute is changed to the secondary volume deletes in the cache memory before recording the drives. Therefore the volume that is changed to the secondary volume goes back to the primary volume before swapping. After that, when a pair deletes from the array with power down with cache volatilization, though a partner of a pair is a primary volume attribute, pair deletion is successful. So the pair deletes as the own array is the primary volume and the other array is the secondary volume, the volume in the other array remains the internal information incorrectly. Moreover, when a pair creates again using the volume that a pair deletes from the array with power down with cache volatilization, a controller is blocked by detecting logic inconsistency because the internal information that should not exist exists incorrectly. And, even if a array power cycle, the same phenomenon occurs again because the incorrect internal information exists on the cache memory. <Countermeasure> The firmware is fixed to delete the pair in the array which delete a pair only when the pair attribute is the primary volume in the remote array for deleting pair.
	9	C	A	-	VB8-0142 (Same as DF850 V17-0093)	Controller is blocked by firmware update with reboot while receiving host I/O.	[Phenomena] Controller is blocked by firmware update with reboot while receiving host I/O. <Web Message> In case that host I/O is received by Fibre Channel interface HJ08xx Microprogram error[FSM] In case that host I/O is received by iSCSI interface HH7Dxy Microprogram error[ISM] <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Host I/O is received. (2) Reboot command is performed from Hitachi Storage Navigator Modular 2 　　(firmware update with reboot, reboot of array system, unlock of Dynamic Provisioning license, or lock of Dynamic Provisioning license) [Probability of failure] Low [Cause] Firmware bug While host I/O operations are being handled by the kernel monitoring, if a interruption occurs due to the reboot instruction, the firmware bug causes host I/O operations to be handled incorrectly during the interruption. After that, inconsistency in host I/O operations is detected by the kernel monitoring, resulting in controller blockage. <Countermeasure> The firmware is fixed to prevent host I/O operations during the interruption due to reboot instructions. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform either (A) or (B) of the following procedures. (A) When controller automatic recovery mode is enabled 　No processing is necessary since blocked controller automatically recovers after phenomenon occurs. (B) When controller automatic recovery mode is disabled. 　Recover the controller by dummy replacing blocked controller. <Web Message> In case that host I/O is received by Fibre Channel interface HJ08xx Microprogram error[FSM] In case that host I/O is received by iSCSI interface

	10	C	A	-	VB8-0141	Controller may be blocked when the SI pair status becomes PSUE (Failure) in Dynamic Provisioning (HDP) and ShadowImage (SI) configuration, or migration fails in HDP and Modular Volume Migration (MVM) configuration.	[Phenomena] Controller may be blocked if intermittent hardware failure of a controller occurs at the same time when the SI pair status becomes PSUE (Failure) in HDP and SI configuration, or migration fails in HDP and MVM configuration. <Web Message> HJ4ABI Microprogram error was detected[HDP](CTL-x) <Equipment model / Firmware version> DF800S/M/H, V7.0/A (0870/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. When HDP and SI are used: (1) HDP is enabled. (2) SI is enabled. (3) The following SI pair exists meeting all of the following conditions. - The pair status is COPY (Synchronizing) or RCPY (Reverse Synchronizing). - P-VOL or S-VOL is DP volume. (4) The status of the pair of (3) becomes PSUE (Failure). (5) Internal reset (CHK1 reset) occurs in the controller immediately after (4) due to the intermittent hardware failure of a controller. [Cause] Firmware bug If CHK1 reset is performed immediately after the pair status becomes PSUE when the copy function accesses the DP volume, the incorrect initial settings for CHK1 reset fails to make the firmware clear the DP volume access flag, causing the copy function to attempt access to the DP volume regardless of the pair status of PSUE after CHK1 reset. This results in controller blockage due to the incorrect copy handling. <Countermeasure> The initial settings for CHK1 reset were fixed to make the firmware clear the DP volume access flag when the pair status is PSUE. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform the following procedures. (1) Dummy-replace the blocked controller. (2) Retry resync or restore if SI is used; retry migration if MVM is used. <Web Message> HJ4ABI Microprogram error was detected[HDP](CTL-x)
	11	C	A	-	VB8QA008	Controller blockage or array system down may occur if a media error occurs on the HDD from which dynamic sparing is performed in the RAID group of RAID 6.	[Phenomena] Controller blockage or array system down may occur if a media error occurs on the HDD from which dynamic sparing is performed in the RAID group of RAID 6. <Web Message> HJ17FF Microprogram error[DRC] <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. (1) RAID 6 (2) Unreadable data (unreadable PIN data) exists in one HDD and another unreadable data (unreadable PIN data) or media error exists on one or more HDDs other than the HDD. These unreadable data (unreadable PIN data) and media error is in the same LBA on each HDD. (3) In the RAID group of (1), dynamic sparing is performed to a HDD other than (2). (4) After dynamic sparing of (3) starts, a media error occurs in reading for dynamic sparing on the HDD from which dynamic sparing is performed. The block of the media error is the first parity (P parity) or the second parity (Q parity) of RAID 6 and in the same LBA of the unreadable PIN data of (2) or the media error.

							[Cause] Firmware bug After dynamic sparing starts, if a media error occurs, the data in the LBA is recovered by correction copy. At this time, if Condition of Occurrence (4) is met, the data recovery operation should skip the LBA and recover the next LBA. However, the firmware bug causes correction copy failing to skip the LBA, resulting in controller blockage due to the incorrect data recovery operation. If the number of media errors do not exceeds the threshold, the other controller is also blocked following the blockage of the controller, resulting in array system down. <Countermeasure> The firmware was fixed to skip the LBA of the media errors and to recover the next LBA. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform the following procedure. For array system down: Turn OFF the main switch, and then turn it ON to boot the array. For controller blockage: Dummy-replace the blocked controller. <Web Message> HJ17FF Microprogram error[DRC]
	12	C	B	-	VB8-0118	The pair status in ShadowImage (SI) or Modular Volume Migration (MVM) may become PSUE (failure) when copy operation is performed after the pair becomes PSUE (Failure) status.	[Phenomena] In the SI or MVM configuration, after the status of the pair in process of copying becomes PSUE (Failure) due to the controller blockage, the pair status may become PSUE (Failure) again when resync or restore is performed if SI is used, or migration is performed if MVM is used. <Web Message> IF0000 Resync failed(LU-XXXX/YYYY) IG0000 PSUE occurred(LU-XXXX/YYYY) XXXX is LUN of P-VOL; YYYY is LUN of S-VOL. <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. When SI is used: (1) SI is enabled. (2) Four or more pairs that are in COPY (Synchronizing) or RCPY (Reverse synchronizing) status exist in each core of one controller. (3) One or more pairs exist that are in COPY (Synchronizing) or RCPY (Reverse synchronizing) status exist in each core of the other controller. (4) To the pair of (3), write access from the host is received by: [Cause] Firmware bug When the pair status becomes PSUE (Failure), the copy function initializes the copy management information. However, if one controller is blocked before the initialization and the other controller is busy handling its maximum number of copy operations, the copy management information fails to be initialized. After that, when the copy operation is performed to the pair whose status has become PSUE, the copy operation is performed based on the copy management information that failed to be initialized, resulting in the pair status becoming PSUE (Failure) when the check is performed at the completion of the copy. <Countermeasure> The firmware is fixed to perform initializing operation when the copy operation is started if the copy operation is performed to the pair whose status is PSUE (Failure). [Recovery] Apply the fixed firmware. <Action in the case of the failure> Recover the blocked controller, and then retry resync or restore. <Web Message> IF0000 Resync failed(LU-XXXX/YYYY) IG0000 PSUE occurred(LU-XXXX/YYYY) XXXX is LUN of P-VOL; YYYY is LUN of S-VOL.

	13	C	B	-	VB8-0143	In the TrueCopyExtendedDistance (TCE) configuration, the pair may not be able to be deleted even if the individual pair deletion is instructed to the pair whose status has become PSEU (Failure).	[Phenomena] In TCE configuration, after the status of a pair has become PSUE (Failure) due to a failure or a pair deletion failure, the pair may not be able to be deleted even if individual pair deletion is instructed. At this time, no error messages are output. <Web Message> None <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) TCE is enabled. (2) TCE pair exists. (3) Individual pair deletion is instructed to the pair of (2). (4) The statuses of all the the pairs in the CTG where the pair (2) belongs become PSUE (Failure) due to one of the following conditions. - Remote path is blocked. - Pair deletion is instructed to the pair other than (3) when the pair status is S-VOL Takeover. (5) Pair deletion is instructed again to the pair of (3) whose status has become PSUE. [Cause] Firmware bug When the Conditions of Occurrence (4) is met during pair deletion, the internal status of the pair is set to "Pair deleting". If the statuses of all the pairs in the CTG have become PSUE, the pair deletion operation is canceled. At this time, the internal statuses remain "Pair deleting." When pair deletion is instructed again later, the firmware bug causes the pair deletion operation to fail, resulting in not being able to delete the pairs. <Countermeasure> The firmware was fixed to perform pair deletion operation if the pair status is PSUE (Failure) and the internal pair status is "Pair deleting" at the time the pair is deleted. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Delete the pair after applying the fixed firmware. <Web Message> None
	14	C	B	-	VB8-0148 (Same as DF850 V20-B035)	A controller is blocked by the instruction of path recovery after controller blockage during updating firmware.	[Phenomena] For TrueCopy remote replication or TrueCopy Extended Distance, a controller blockage occurs by some cause during updating firmware. Then, after recovering the controller, when the path recovery is executed, the following phenomena occur. (a) The controller which executes path recovery is blocked. (b) The path recovery fails. <Web Message> (a) HH7EEJ Microprogram error[ILM] (b) HJ091D Microprogram error[ILM] <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] <Case 1> The problem may occur when all of the following conditions are met. (1) TrueCopy remote replication or TrueCopy Extended Distance is installed. (2) iSCSI is used for the remote path. (3) Execute firmware update. (4) While (3), a controller is blocked and then is recovered. (5) By (4), the remote path is blocked. (6) For the remote path of (5), the path recovery is executed via the

							[Cause] Firmware bug While the firmware update, the path recovery processing uses exclusive processing. An exclusive flag is used to decide whether the firmware is updating and the flag management has bug. When a controller is blocked during updating firmware, the firmware update is completed by the controller recovery but the flag is not OFF. So when the path recovery is executed, the exclusive processing for the firmware update works. Therefore the path recovery fails in the case of Fibre Channel and a controller is blocked in the case of iSCSI. <Countermeasure> The firmware is fixed to do the update firmware flag in OFF for the path recovery when a controller is blocked. [Recovery] Apply the fixed firmware. <Action in the case of the failure> When the controller is blocked, recovery the controller and then power cycle the array. <Web Message> HH7EEJ Microprogram error[ILM] or HJ091D Microprogram error[ILM]
	15	C	B	-	VB8-0150	HDD may be blocked when the array is booted after the power down without cache volatilization or a controller is blocked during the DP pool format.	[Phenomena] HDD may be blocked when the array is booted after the power down without cache volatilization or a controller is blocked during the DP pool format. <Web Message> IY0F00 LA error[errcode:LUN](Unit-X,HDU-Y) <Equipment model / Firmware version> DF800S/M/H, V7.0/A (0870/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Dynamic Provisioning is enabled. (2) DP pool exists meeting all of the following conditions. - SATA HDD comprises it. - RAID level is RAID 5 or RAID 6. (3) DP pool format is performed in the DP pool of (2) DP pool format is triggered by the following events. - DP pool creation - DP pool reinitialization - DP pool capacity addition - Virtual LU format - Virtual LU deletion - Virtual LU shrinkage - DM-LU release (4) Power down without cache volatilization or controller [Cause] Firmware bug After power down without cache volatilization or controller blockage occurs while the DP pool format data is being created, the firmware tries to search and discard the format data in the middle of creation when the array is booted or jobs in the blocked controller are handed. But the firmware bug may cause the correct search and discard to fail. In this case, the firmware reads the unformatted space on the drive to create complete format data, resulting in the SATA HDD blockage. <Countermeasure> The firmware was fixed to correctly search and discard the DP pool format data in the middle of creation when the array is booted after power down without cache volatilization or jobs in the blocked controller are handed. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Replace the blocked HDD. <Web Message> IY0F00 LA error[errcode:LUN](Unit-X,HDU-Y)

	16	C	B	-	VB8-0114	Host I/O may be stopped during resetting of the controller B (CHK1 reset) occurred after the controller A is replaced.	[Phenomena] Host I/O may be stopped during resetting of the controller B (CHK1 reset) occurred after the controller A is replaced. <Web Message> HJ0764 Microprogram error[FTD] <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) FC Port is used. (2) Controller A is blocked. (3) LU whose ownership is owned by the core of the controller A of (2) receives the host I/O (cross call I/O) from the FC port of the controller B opposite to (2) immediately before the blockage of the controller A is started. (4) The controller A of (2) is recovered by replacing the controller A. (5) Host I/O operations as in (3) are received; or connect and disconnect the FC cable of the FC port of (3). [Probability of failure] Low [Cause] Firmware bug When the LU whose ownership is owned by the core of the controller A receives cross call I/O from the FC port of the controller B, FC protocol chip of FC port may pause this cross call I/O. After that, Condition of Occurrence (5) causes the FC protocol chip to restart the I/O operation. At this time, the FC protocol chip should discard this I/O because the I/O is invalid due to the blockage of the controller A, but the firmware bug causes CHK1 reset to occur in the controller B recognizing it to be invalid I/O. During the CHK1 reset, host I/O stops. <Countermeasure> The firmware was fixed to make the FC protocol chip control operation to discard the cross call I/O that has become invalid due to the controller blockage. [Recovery] Apply the fixed firmware. <Action in the case of the failure> No action is required because the controller reset (CHK1 rest) occurs only once. <Web Message> HJ0764 Microprogram error[FTD]		
	V11.7/P, 08B7/P							9/14/2012	433 -
V11.7/P 08B7/P Base System V11.7/N 08B7/N	1	C	A	SD4744973	VB8-0156	Host access or changing settings with HSNM2 may fail after changing settings with HSNM2 in local array fails following a network channel failure of remote path in the TrueCopy configuration.	[Phenomena] After a network channel failure in TrueCopy configuration, the following phenomena may occur. (Phenomenon 1) Host access or changing settings in local array may fail after failing to change settings with Hitachi Storage Navigator Modular 2 (HSNM2) in local array. (Phenomenon 2) Host access to LU whose ownership failed to change after load balancing performs LU ownership change, or to P-VOL of TrueCopy Extended Distance (TCE) or SnapShot (SS), etc may fail temporarily. This phenomenon occurs every time load balancing operates. <Web Message> None <HNSM2 Message> [DMEA000006] Failed to connect with the subsystem. Confirm the subsystem status and the LAN environment, and then try again. <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. (1) TrueCopy remote replication (TC) or TCE is enabled.		

							[Cause] Firmware bug TrueCopy initiator function sends ABTS command to remote array to suspend SCSI commands that time out. When the ABTS command times out too, TrueCopy initiator function send PLOGI command to remote array to rest all the TrueCopy SCSI commands, but the firmware bug causes the reset of the SCSI command that has timed out to fail if remote array receives PRLO command, or Link down occurs in the remote path before remote array receives PLOGI command. If unresettable SCSI commands continue to remain, changing settings with HSNM2 becomes impossible after that. In addition, host access to the LU whose ownership fails to change every time load balancing operates, or to P-VOL of TCE or SS, etc. may temporarily become impossible. <Countermeasure> The firmware has been fixed to make TrueCopy initiator rest SCSI commands when remote array receives PRLO command, or Link down occurs in the remote path. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform the following. (1) Dummy-replace the controller where host access fails. Dummy-replace the controller where changing setting with HSNM2 fails.			
	2	C	A	SD4775118	VB8-0157	Array system down may be caused by subsequent blockage of controller #1 due to a intermittent hardware failure and a intermittent 10Gbps iSCSI interface failure occurred simultaneously after blockage of controller #0.	[Phenomena] Array system down may be caused by subsequent blockage of controller #1 due to a intermittent hardware failure and a intermittent 10Gbps iSCSI interface failure occurred simultaneously after blockage of controller #0. <Web Message> HHA110 iSCSI firmware load failed <Equipment model / Firmware version> DF800H/EH, V11.0/A (08B0/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) DF800H or DF800EH (2) 10Gbps iSCSI interface is used. (3) Controller #0 is blocked. (4) An intermittent hardware failure occurs in controller #1 after (3). (5) An intermittent 10Gbps iSCSI interface failure occurs while controller #1 is being recovered (CHK1 reset of controller is being performed). [Probability of failure] Low <Explanation> This problem occurs when all the conditions are met, but when [Cause] Firmware bug When CHK1 reset in controller #1 is performed during blockage of controller #0, the firmware bug incorrectly refer to the reset status of iSCSI interface of controller #0 to set the reset status of the iSCSI interface to "Resettable". After that, when a iSCSI failure occurs while iSCSI Firmware is being loaded, the iSCSI interface is incorrectly soft reset because the reset status is "Resettable". This causes loading iSCSI Firmware to fail, resulting in array system down. <Countermeasure> The firmware has been fixed to correctly refer to the reset status of the iSCSI interface of controller #1 to set the reset status of the iSCSI interface of controller #1 to "Unresettable" when CHK1 reset is performed in controller #1 during blockage of controller #0. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Turn OFF the main switch, turn it ON, and then reboot the array. <Web Message> HHA110 iSCSI firmware load failed			
	V11.7/S, 08B7/S							11/7/2012	436	033

V11.7/S 08B7/S Base System V11.7/P 08B7/P	1	C	A	SD4627254, SD4837659	VB8-0166	SAS HDD blockage or access lost may occur when online firmware exchange is performed on SAS and SATA mixed configuration during heavy duty access.	[Phenomena] Some SAS HDDs may report 02/0401 (Becoming ready) error after 06/2904 (Internal reset) report when online firmware exchange is performed on SAS and SATA mixed configuration during heavy duty access, and then SAS HDD blockage or access lost may occur. <Web Message> Normal HDD blockade case IY0000 HDU error report(Unit-x, HDU-y)[02-0401] W09zab HDU alarm (Unit-x, HDU-y, Type-c) Multiple HDD failure case I30100 HDU error (Unit-x, HDU-y) I41700HDU error over (Unit-x, HDU-y)[IFUNR] <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later HDD Products/Version: DF-F800-AKH600/AKH600X/AKH450/AKH450X/AKH300/AKH146, D02D and before [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) The specified HGST SAS HDD is mounted. (Note1) (2) The HDD FW is D02D and before. [Cause] HDD firmware bug An internal reset may occur in the HDD due to the HDD firmware bug when an HDD operates ATI (Adjacent Track Interference) prevention in Idle state and receives LUN reset from array controller ahead of I/O at the same time. An HDD transits to Idle state when an access to the HDD stops for more than 0.5 second. ATI prevention is performed under specified conditions in the Idle state. The HDD firmware bug may appear in ATI prevention process with specified conditions. The array firmware blocks the HDD if 02/0401 (Becoming Ready) is sent during I/O. If internal reboots occur in multiple HDDs in single RAID group, the array firmware cannot respond to the host until internal reboots are finished. <Countermeasure> HDD firmware was fixed to operate LUN reset preventing internal reset even if confliction between ATI Prevention and LUN reset occurs. [Recovery] Perform online firmware exchange with array firmware bundled the fixed HDD firmware after online drive firmware update according to FCB DF800-033. (Note1)	
	V11.7/U, 08B7/U							11/16/2012　437　034
V11.7/U 08B7/U Base System V11.7/S 08B7/S	1	C	B	None	VB8-0168	HDD response delays may occur temporarily at drive firmware update.	[Phenomena] (Phenomena1) When online drive firmware update for HGST SAS HDDs (*1) is performed, response delays (for a maximum of 16 seconds) of read access for the LUs of the HDDs may occur temporarily. Also, it may take longer than expected to complete online drive firmware update because it takes maximum 16 seconds longer than expected to reboot an HDD per one HDD. (Phenomena2) When the new firmware executes automatic drive firmware download for HGST SAS HDD (*1) after the array firmware update, response delays (for a maximum of 16 seconds) of read access for the LUs of the HDDs may occur temporarily. (*1) DF-F800-AKH600(H),AKH600X(H),AKH450(H1),AKH450X(H1),AKH300(H2),AKH146(H2) <Web Message> None <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later HDD Products/HDD Firmware Version: DF-F800-AKH600(H)/AKH600X(H)/AKH450(H1)/AKH450X(H1)/AKH300(H2)/AKH146(H2), D02E and before	

							[Cause] HDD firmware bug When the HDD firmware receives the HDD reboot command to activate the new HDD firmware and the confliction between the HDD reboot command and the ATI Prevention processing occurs, the HDD firmware may not abort the ATI Prevention processing due to the HDD firmware bug. At that time, it takes longer than expected to complete online drive firmware update or response delays of read access for the LUs of the HDDs occur because the HDD does not reboot until the ATI Prevention processing is completed. <Countermeasure> The HDD firmware was fixed to abort the ATI Prevention processing when an HDD receives the HDD reboot command of drive firmware update during the ATI Prevention processing. [Recovery] Perform online firmware exchange with the array firmware bundled with the fixed HDD firmware after online drive firmware update according to FCB DF800-034. (Note1) Note1: If online firmware exchange is performed without online drive firmware update, the problem may appear slightly. <Action in the case of the failure> None (Wait for online drive firmware update to be completed even if it takes longer than expected.)				
	V11.7/V, 08B7/V							11/30/2012	439	-
V11.7/V 08B7/V Base System V11.7/U 08B7/U	1	I	-	SD4809286/DF800-32391, SD4929469/DF800-32816	VB8-0167	Improvement in response sending at Fibre Channel(FC) path failure	In an FC interface (I/F) configuration, when many response timeout errors and link down occur due to an FC path failure, the FC protocol chip in an FC I/F may become unable to complete sending a response, resulting in depleting internal resources for sending responses to cause an FC I/F port to become unresponsive to hosts. To address this, the firmware is improved to check the status of response sending and if it detects a response that is not completed, it resets the FC protocol chip to prevent a port from being unresponsive.			
	2	I	-	None	VB8-0162	Improvement in responding to login commands at host boot	In a Fibre Channel configuration, login commands (PLOGI command) may be issued by an HBA to each logical unit (LU) at host boot. If many LUs are mapped, it may take a long time for a host to boot. To address this, new port option "PLOGI Response Quick Mode" is supported for an array to respond preferentially to login commands to reduce the time spent by a host to boot. This mode is available in Hitachi Storage Navigator Modular 2 version 11.78 and later. You can enable the mode if it takes a long time for a host to boot due to a large number of login commands issued as above.			
	3	C	A	SD4864781/DF800-82458, SD4693304/DF850-32042	VB8-0161 (Same as DF850 V30-0434)	Controller blockage caused by many retries of packet sending when secure communication is used.	[Phenomena] When secure communication is used between an array and management software (Hitachi Storage Navigator Modular 2 (HSNM2), Hitachi Device Manager, etc.), a controller may be blocked due to many retries of packet sending. <Web Message> HZ0N00 Kernel Processing error <Equipment model / Firmware version> DF800S/M/H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Secure communication is used in management software (Secure port of the array is accessed by HSNM2, etc.) (2) Communication packet is sent again in the network. [Probability of failure] Low <Explanation> This problem occurs only when the receiving process triggered by receiving command termination notification in the specific order and the packet resending process occur at the same time. In the actual environment, it occurred about once in one month in the LAN where 4% packets were lost.			

							[Cause] Firmware bug In the LAN where communication quality is degraded to cause communication packets to be resent, the Secure communication process may terminate the Secure communication even if it is yet to be completed (if LAN command termination notification is received in the specific order). In this process, the firmware bug causes termination of the Secure communication without suspending the resending. Because of this, the Secure communication resending process incorrectly accesses the memory regardless of the released status of the memory for the Secure communication, resulting in the incorrect memory access being detected to block a controller. <Countermeasure> The firmware has been fixed to terminate the Secure communication after suspending the resending process while packets are being resent. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy-replace the blocked controller. <Web Message> HZ0N00 Kernel Processing error			
	4	C	A	None	VB8-0164/0163 (Same as DF850 V30-B010/V25-B025)	Controller blockage in local array caused by timeout due to FC path failure, etc. in TrueCopy remote replication(TC) or TrueCopy Extended Distance(TCE).	[Phenomena] In the TC or TCE configuration where arrays are connected with a Fibre Channel (FC) interface, if command timeout occurs due to a FC path failure, etc., a controller may be blocked in the local array. <Web Message> HJ099B Microprogram error[LSM] or HJ0832 Microprogram error[FSM] <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Fibre Channel (FC) interface is used. (2) TC or TCE is enabled. (3) A remote path is configured in an FC interface. (4) Local array in TC or TCE (5) Two or more pairs of (2) exist. (6) Among the pair LUs of (5), the core(A) has the LU ownership of the pair LU(A) and the core(B) has the LU ownership of the pair LU(B). (7) In the pair of LU(A), a TrueCopy SCSI command sent from the core(A) to a remote array times out due to a remote path failure, etc. The core(A) sends an ABTS command to a remote			
							[Cause] Firmware bug If a TrueCopy SCSI command times out, a local array sends ABTS (abort command) to a remote array. At this time, the ABTS sending process changes the sending status of the ABTS command. However, if a prioritized PLOGI sending process is triggered during this change process, the firmware bug causes the PLOGI sending process to incorrectly change the sending status of the ABTS command instead of the ABTS command sending process. This causes detection of the incorrect sending status of the ABTS command by the ABTS sending preparation process, resulting in controller blockage. <Countermeasure> The firmware has been fixed to ensure that a prioritized PLOGI sending process does not change the sending status of an ABTS command. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy-replace the blocked controller. <Web Message> HJ099B Microprogram error[LSM] or HJ0832 Microprogram error[FSM]			
	V12.1/A, 08C1/A							2/7/2013	448	-
V12.1/A 08C1/A	1	N	-	None	VC2-0001	TrueCopy Modular Distributed (TCMD) is enhanced.	Connecting DF800 to DF850 using TCMD is supported.			

Base System V11.7/V 08B7/V	2	I	-	SD4870509/DF800-32548	VC2-0002	Improvement in Online Drive Firmware update function	While drive firmware is being transferred to an array with the "Executing" dialog box of Installation of Drive Firmware Program, if the "Drive Firmware Information" button in the "Drive Firmware Install" screen is clicked, the Installation is suspended in a running state. After this, if the "Install" button is clicked, the Installation causes an error with the following Dialog message. The firmware is improved to perform Installation by clicking the "Install" button again at this time. <Dialog Message> 1006: Subsystem is Executing Other Event.
	3	I	-	DF800-30778 (RASR0091)	VC2-0011	Improvement in Drive Error Information management	At the beginning of Array boot up process, the bits of Drive Error Information (Page Code 33h) are once all cleared (bit OFF). Then the Array comes Ready status and when it detects dual HDDs failure (RAID5) or triple HDDs failure (RAID6), it sets their bits of Drive Error Information again (bit ON). At this time, WEB information message of "I30100 HDU error" is reported. According to above logic, the Online Firmware Upgrading process for this new Firmware version can NOT reflect this new improved logic by itself, but the Array reboot process is also necessary. [Additional notice] The status bit ("Drive Error") for each failing HDD is set when the HDD is detected to have failed such that the failed HDD could cause an access loss to the raid group from the hosts. Hi-Track checks these bits and will indicate an error condition and open a case if any bits are on. There have been some incidents in the field where these status bits were turned on for many of the HDDs in a system due to an incorrect installation procedure where the HDDs were changed from their shipped locations and where that status wasn't properly cleared afterwards by the person doing the installation. Maintenance personnel are supposed to do either of the following procedures to correct the situation - 1) Correct the locations of HDDs/cablings, etc. so that the HDDs are located as they were configured at the build center. 2) Perform an initial setup. This error condition occurs if the maintenance personnel simply delete the raid group and brings the system up to the Ready status rather than perform the correct procedures above. Leaving the
	4	I	-	None	VC2-0008 (Same as DF850 V35-0063)	Improvement in Dynamic Provisioning management information management method	The firmware is improved to manage the Dynamic Provisioning management information with two sides of new and old information. This enables DP Pool to be used with the old management information without formatting all the DP Pool data by the firmware if power down with cache volatilization occurs and the new management information becomes unavailable in an array while the management information is being updated in HDD
	5	C	A	SD4908513/DF850-82507	VC2-0014 (Same as DF850 V35-0107)	Remote path may be blocked or array may become unresponsive to host with iSCSI interface configuration.	[Phenomena] If a temporary iSCSI interface board failure and a temporary controller failure occur at the same time, iSCSI interface board goes link down to become unable to recover and the following phenomena may occur. (Phenomenon 1) In TrueCopy remote replication(TC) or TrueCopy Extended Distance(TCE), if local and remote arrays are connected via Switch, and a remote path is set in an iSCSI interface, the remote path is blocked. At this time, the port of the iSCSI interface of the local array goes link down. (Phenomenon 2) In TC or TCE, if local and remote arrays are directly connected, and a remote path is set in an iSCSI interface, the remote path is blocked. (Phenomenon 3) In TC or TCE, if a remote path is set in an iSCSI interface, the remote path is blocked. At this time, the port of the iSCSI interface board goes link down. (Phenomenon 4) The array becomes unresponsive to a host in the array where host I/O operations are processed with an iSCSI interface. <Web Message> (Phenomenon 1)

							[Cause] Firmware bug If a failure occurs in the iSCSI protocol chip, the iSCSI protocol chip control process resets the chip. When a controller failure is detected during the reset, the firmware bug causes the iSCSI protocol chip control process to perform another reset to the chip even if the reset is being performed. This causes chip reset management information to become inconsistent with the chip becoming unable to recover from the reset status, resulting in a remote path blockage or an array unresponsive to a host with iSCSI port remaining link down. <Countermeasure> The firmware has been fixed to ensure that the iSCSI protocol chip control process does not perform another reset if the chip is being reset at the time of the detection of a controller failure. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy-replace the controller of the local array where a remote path is blocked or the controller that becomes unresponsive to a host. (In Phenomenon 1, dummy-replace the controller of the local array where the port of an iSCSI interface goes link down.) <Web Message> (Phenomenon 1)
	6	C	A	None	VC2-0018 (Same as DF850 V35-0113)	Controller may be blocked at online firmware update.	[Phenomena] In iSCSI configuration, if a controller is blocked while its firmware is being updated at online firmware update, recovered by service personnel, and then performed online firmware update again, the controller other than the recovered one may be blocked. <Web Message> HH7ED4 Microprogram error[ILM] <Equipment model / Firmware version> DF800S/M/H, V4.3/A(0843/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) An iSCSI interface is used. (2) One or more hosts are connected to an array with an iSCSI interface. (3) Online firmware update is performed. (4) In the iSCSI port installed in the controller whose firmware is being updated during (3), reset of the iSCSI login information is caused by the following - Removal/insertion of iSCSI interface cable - Log out - Link down, link up - Temporary iSCSI protocol chip failure (5) The controller is blocked whose firmware is being updated during the reset of (4). [Cause] Firmware bug If Condition of Occurrence (4) is met, the iSCSI login process of the controller B, which is in operation, resets the iSCSI login information of the port of the controller A, whose firmware is being updated. If the controller A is blocked at this time, the reset initiation time is recorded in the iSCSI login information in the controller B. When online firmware update is performed again after the controller A recovered, the iSCSI login process of the controller B refers to the reset initiation time without initializing it to cause reset timeout, resulting in blockage of the controller B. <Countermeasure> The firmware has been fixed to ensure that the iSCSI login process initializes the reset initiation time of the iSCSI login information when online firmware update is initiated. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Follow these steps. (1) Dummy-replace the blocked controller. (2) Perform online firmware update again. <Web Message> HH7ED4 Microprogram error[ILM]

	7	C	A	None	VC2-0023	Controller may be blocked if DP pool reinitialization is performed.	[Phenomena] Controller may be blocked if DP pool reinitialization is performed. <Web Message> HJ37H3 Microprogram error[DMI] or HJ37BA Microprogram error[DMI] <Equipment model / Firmware version> DF800S/M/H, V8.0/A(0880/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Dynamic Provisioning is enabled. (2) A DP pool has been created. (3) A DP pool exists that consists of multiple DP RAID groups. (4) Perform pool reinitialization to the DP pool of (3). [Probability of failure] Low <Explanation> Its occurrence depends on the timing when the management information is moved between DP RAID groups and periodical destage is completed at the same time. [Cause] Firmware bug If the DP management information is stored in the DP RAID group A, where DP pool reinitialization is executed, the DP management information destage process moves it to the DP RAID group B. At this time, if periodical destage of the DP management information (stored in the DP RAID group A at this time) to an HDD is completed, the DP management information destage process incorrectly determines that the DP management information is incorrectly moved, resulting in controller blockage. <Countermeasure> The firmware has been fixed to ensure that the DP management information destage process determines that the DP management information is correctly moved if it is moved between DP RAID groups and periodical destage is completed at the same time. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy-replace the blocked controller. Note that you should not perform pool reinitialization until the controller recovers (while the controller is blocked) because array system down may be caused. <Web Message> HJ37H3 Microprogram error[DMI] or HJ37BA Microprogram error[DMI]	
	8	C	A	None	VC2-0005	Controller may be blocked at HDD media error.	[Phenomena] When the online verify (HDD media diagnosis) process detects an HDD media error, a controller may be blocked. If the array model is DF800H or DF800EH, the other controller also may be blocked to cause array system down. <Web Message> HJ11D0 Microprogram error[RCH] <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] A controller blockage occurs when all of the following conditions are met. (1) One of the following is met. (1-1) Two or more normal LUs are created. (1-2) Alternatively, two or more virtual LUs are created in one DP Pool. (2) An HDD media error is detected by the online verify process. (3) One of the following is met. (3-1) The error block of (2) is assigned to the normal LU(A) (Ownership: Controller A) (Note 1) and the subsequent block is assigned to the normal LU(B) (Ownership: Controller B) (Note 1). (3-2) The error block of (2) is assigned to the virtual LU(A) (Ownership: Controller A) (Note 1) and the subsequent block is assigned to the virtual LU(B) (Ownership: Controller B) (Note 1).	

							[Cause] Firmware bug If an HDD media error is detected by the online verify process, it also diagnoses the subsequent block to facilitate error detection. At this time, an illegal access causes a controller blockage if the subsequent block is assigned to the LU that is owned by the other controller (DF800H/EH: the other core) because the online verify process fails to check the LU ownership. In DF800H/EH, if the other controller experiences this phenomenon, array system down is caused. <Countermeasure> The firmware has been fixed to ensure that the online verify process does not diagnose the block if it is subsequent to a block where media error occurs and assigned to the LU that is owned by the other controller (DF800H/EH: the other core). [Recovery] Apply the fixed firmware. <Action in the case of the failure> - At controller blockage Follow these steps. (1) Disable online verify ([Configuration Settings]-[Online Verify]-[Online Verify Test]-[Enable Online Verify] in Hitachi Storage Navigator Modular 2 GUI). (2) Dummy-replace the blocked controller. (3) Install the fixed firmware in an updating manner (4) Enable online verify
	9	C	B	SD4804615/DF800-32354, EUC1701501/DF800-55644	VC2-0003 (Same as DF850 V30-0466)	Online drive firmware update procedures may fail with error termination.	[Phenomena] Online drive firmware update procedures may fail with error termination regardless of the Ready status of the array. <Dialog Message> 1008: subsystem is down <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] Condition 1 The problem occurs when all of the following conditions are met. (1) Block one controller by pressing RET SW at preventive replacement, etc. (2) Replace or dummy-replace the controller of (1) after (1). (3) Perform the following after the array has not been performed planned shutdown, restart, or reboot since (2). (3.1) Perform (1)(2) to the counterpart of (1). (3.2) Perform Online drive firmware update procedures after (3.1). Condition 2 The problem occurs when all of the following conditions are met. (1) Block controller #0 by pressing RET SW at preventive replacement, etc. (2) Replace or dummy-replace the controller #0 after (1). (3) Perform the following after the array has not been performed [Cause] Firmware bug When the controller A goes into Maintenance Mode, the value indicating "Controller A unavailable" is registered in the management information by the WEB function, but it may also registered in that of the controller B due to the firmware bug. In this case, this value is kept in the management information of the controller A when it recovers. This value causes Online drive firmware update to fail after it is instructed to the controller A. Note The WEB management information is initialized at planned shutdown, restart, or reboot of the array. <Countermeasure> The firmware has been fixed to ensure that the WEB process registers the value indicating "Controller unavailable" only in the management information of the controller that is in Maintenance Mode. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform one of the following. (1) Use Memory Maintenance Tool (ECN HUS-DFUTL-208) in the array. (2) Planned shutdown the array and restart it. (3) Reboot the array.

	10	C	B	SD4901239/DF800-82482	VC2-0007	In Forced Parity Correction, its status may incorrectly become "Normal" (complete) instead of "skipped" when "Skip Parity Correction" is instructed.	[Phenomena] After power down with cache volatilization occurs in an array that has a DP Pool consisting of multiple RAID groups, restart the array. After it starts, an HDD constituting the DP pool is blocked to trigger correction copy. After this, if "Skip Parity Correction" in Forced Parity Correction is executed, the following occur. The consistency between the data in the DP RAID group that was not the target of correction copy and the parity data can not be guaranteed. - If "Skip Parity Correction" is executed before correction copy is complete. The virtual LU status of Forced Parity Correction becomes "skipped", but it changes incorrectly from "skipped" to "Normal" (complete). - If "Skip Parity Correction" is executed after correction copy is complete. The virtual LU status of Forced Parity Correction becomes incorrectly "Normal" (complete) instead of "skipped". <Web Message> None <Equipment model / Firmware version> DF800S/M/H, V7.0/A (0870/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. [Cause] Firmware bug At the completion of the correction copy of an HDD of RAID 1 or RAID 5, the forced parity correction process incorrectly recognizes that its status can be changed to "Normal" without checking whether "the recovered LU is a virtual LU" and "the DP Pool where the LU belongs consists of multiple RAID groups". This results in the status becoming "Normal", which should be "skipped", after the correction copy is complete or "Skip Parity Correction" is instructed. <Countermeasure> The firmware has been fixed to keep the forced parity correction status of a virtual LU as "skipped" if the recovered LU is a virtual LU and the DP Pool where it belongs consists of multiple RAID groups at the completion of the correction copy of an HDD of RAID 1 or RAID 5. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform Forced Parity Correction to the LU that is indicated in the following Web Message. <Web Message> W0R000 User data lost(LU-x)	
	11	C	B	SD4947020/DF800-32882	VC2-0017	A 10Gbps iSCSI interface becomes unresponsive to ICMP command (Ping) sending packets under 18 bytes.	[Phenomena] When an ICMP command is issued from a host to a 10Gbps iSCSI interface with the packet size set to 17 bytes or less, the array becomes unresponsive to the command. <Web Message> None <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.0/A(08B0/A) and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. (1) A 10Gbps iSCSI interface is used. (2) An ICMP command is issued from a host to the port of (1) with the packet size set to 17 bytes or less. [Probability of failure] High <Explanation> This problem occurs when Conditions of Occurrence are met.	

							[Cause] 10Gbps iSCSI Protocol Chip Firmware bug If the 10Gbps iSCSI Protocol Chip receives an ICMP command whose packet length is 17 bytes or less, the packet is padded to 18 bytes. However, the firmware bug in the packet length check process causes packet length inconsistency to be detected to discard the packet. This results in the 10Gbps iSCSI interface being unresponsive to the ICMP command. <Countermeasure> The 10Gbps iSCSI Protocol Chip Firmware has been fixed to ensure that the packet length check process correctly recognizes the length of the padded packet to be 18 bytes. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Set the packet size of the ICMP command (Ping) to 18 bytes or more in a host. <Web Message> None
	12	C	B	SD4938845/DF800-32853	VC2-0021	DP pool format may not be completed if pool reinitialization is performed in DP pool.	[Phenomena] DP pool format may not be completed if pool reinitialization is performed in a DP pool. After that, DP pool format is not completed even if the following are performed. - Format the virtual LU of the above DP pool. - Delete the virtual LU of the above DP pool. - Add a DP RAID group to a DP pool. <Web Message> None <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.0/A(08B0/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Dynamic Provisioning is enabled. (2) One of the following is met. (2-1) Pool reinitialization is performed to a DP pool that consists of multiple DP RAID groups. (2-2) Pool reinitialization is repeated successively to multiple DP pools. [Probability of failure] Low <Explanation> [Cause] Firmware bug The DP pool reinitialization process performs format by deciding the Chunk range and the target Chunk of format for each DP RAID group while updating the format position (NEXT pointer) according to the progress of format for each DP RAID group. However, if multiple NEXT pointers are updated simultaneously in reinitialization of multiple DP RAID groups, the reinitialization process updates a NEXT pointer with incorrect value. This results in the format being unable to progress due to the incorrect NEXT pointer. <Countermeasure> The firmware has been fixed to ensure that the DP pool reinitialization process correctly updates NEXT pointers even if multiple NEXT pointers are updated simultaneously. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform planned shutdown of the array and perform one of the following. (A) Dummy-replace the controller #0 and controller #1 in turn. (B) Apply the fixed firmware with online firmware update. <Web Message> None

	13	C	B	SD4677516/DF850-32099	VC2-0013 (Same as DF850 V20-0057)	LAN port may become unresponsive when SNMP Agent Support Function (SNMP) is enabled without SNMP configuration file being registered.	[Phenomena] If SNMP is enabled and the SNMP configuration file (CONFIG.TXT) is not registered in the array, user LAN port and maintenance LAN port may become completely unresponsive. In this case, functions such as Hitachi Storage Navigator Modular 2, maintenance WEB, and E-mail alert function are completely unavailable. However, processes unrelated to LAN communication like host I/O operate normally. <Web Message> None <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) SNMP is enabled. (2) SNMP configuration file (CONFIG.TXT) is not registered in the array. (3) Many broadcasted SNMP accesses are received by the array. (Some network appliances may process broadcasted SNMP accesses.) [Probability of failure] Low [Cause] Firmware bug When the array where SNMP is enabled and SNMP configuration file is not set receives broadcasted SNMP accesses, the firmware bug in the network process causes buffers for UDP packets to be depleted to fail LAN tasks. This results in TCP/UDP packets being unable to be processed. <Countermeasure> The firmware has been fixed to ensure that the network process use less buffers to prevent them from being depleted when it receives broadcasted SNMP accesses. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Follow these steps. (1) Disconnect the LAN cables that are connected to user LAN port and maintenance LAN port. (2) Planned shutdown the array, and then restart the array. (3) Connect HSNM2 server directly to user LAN port or maintenance LAN port. (4) Configure SNMP if used, or disable it if not used. (5) Connect the disconnected LAN cables to user LAN port and maintenance LAN port. <Web Message> None		
	14	C	B	None	VC2-0009	Planned shutdown of local array may not be completed when iSCSI interface is used in TrueCopy remote replication (TC) or TrueCopy Extended Distance (TCE).	[Phenomena] When planned shutdown is performed in the local array with an iSCSI interface used in TC or TCE, it may not be completed with the array being unable to be turned off. <Web Message> None <Equipment model / Firmware version> DF800S/M/H, V4.3/A(0843/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) TC or TCE is enabled. (2) A remote path is set in an iSCSI interface. (3) Planned shutdown is performed in the local array. [Probability of failure] Low <Explanation> Its occurrence depends on the timing when a remote copy command is received and the iSCSI protocol chip is reset at the same time.		

							[Cause] Firmware bug When planned shutdown is performed, the iSCSI command process instructs the iSCSI protocol chip to cancel a command, and then clear the command job. At the same time, the iSCSI protocol chip control process resets the chip. However, if planned shutdown is performed immediately after a response to a remote copy command is received, the iSCSI command process fails to clear the command job waiting for the command cancellation to be completed. This results in the command job remaining, with the planned shutdown being unable to be completed. <Countermeasure> The firmware has been fixed to ensure that the iSCSI command process to correctly cancel a command and clear the command job if a command response has been received at planned shutdown. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Follow these steps. (1) Perform power down without cache volatilization. (2) Start the array. (3) Perform planned shutdown of the array. <Web Message> None			
	V12.3/A, 08C3/A							3/15/2013	454	-
V12.3/A 08C3/A Base System V12.1/A 08C1/A	1	N	-	DF800-32819	VC4-0006	Additional browser support	The following platforms are supported in the WEB. Windows 7: Internet Explorer 8.0, 9.0 and 10.0 Windows Vista: Internet Explorer 9.0 Windows 2008: Internet Explorer 9.0			
	2	C	A	EUC1814524/ DF850-55961, SD5107510/ DF850-33450	VC4-0017 (Same as DF850 V37-0161)	After the host executes the XCOPY Command, when the host executes the other commands, a controller is blockaded. When this issue occurs on both controllers, array system down occurs.	[Phenomena] After the host executes the XCOPY Command, when the host executes the other commands, a controller is blockaded. When this issue occurs on both controllers, array system down occurs. <Web Message> HZ0N0X Kernel processing error(CTL-X) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.3/A(0893/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Dynamic Provisioning is enabled. (2) There is a LU that meets all of the following conditions. - It is a DP-VOL - The RAID level of the DP pool with the LU is RAID 5 or RAID 6 - The number of the data drive of the DP pool with the LU is not 1D, 2D, 4D, 8D or 16D. - The LU is not part of ShadowImage, SnapShot, TrueCopy, TrueCopy Extended Distance or Modular Volume Migration pair. (3) Any host executes XCOPY command (*1) for the LU of (2). (4) On XCOPY command of (3), the destination LU is same as the source LU. (5) On XCOPY command of (3), the specified length is that meets one of the following conditions. - If the LU's stripe size is 64KB, the command length is from [Cause] Firmware bug The commands received from hosts obtain resources of cache. Then, the resources of cache obtained, are locked for mutual exclusion. The locking status is managed by queuing. Completing the processing of commands, the lock is released. When the source and the destination area go across page boundary of a DP-VOL, they are locked separately. As a result, XCOPY command may locks up to 3 resources of cache. When fail to lock any resources of cache, need to unlock the resources of cache that is already locked. But, in the case of that third locking is failed after two locking is succeeded there is a firmware bug that the obtained locks are not released incorrectly. If other commands are kept receiving while unreleased locks remain, an internal queue to manage locks becomes a loop. Then, if the queue with a loop is searched, the search never completes and a controller is blocked. Although queues are maintained per controller, if the same situation occurs on the other controller after a controller is blocked, the array goes down. <Countermeasure> Change to unlock all rthe resources of cache that is already locked, in the case of locking failure. [Recovery] Apply the fixed firmware. <Action in the case of the failure>			

	3	C	A	None	VC4-0007 (Same as DF850 V37-0156)	Pair status may fail to become Failure regardless of cache data DMA transferring error during cycle copy in TrueCopy Extended Distance (TCE).	[Phenomena] Pair status may fail to become Failure if a cache data DMA transferring error (DRR(Data Recovery Reconstruction) error) occurs when write access is executed to P-VOL during TCE cycle copy. <Web Message> Messages output when a DRR error occurs: Parity generation LA error[DRR] Parity generation LA error[DRR](CTL-x,DMA-yy) DMA error was detected(CTL-x,DMA-y) ECC write parity error(CTL-x,DMA-y) ECC generate error(CTL-x,DMA-y) ECC correction failed(CTL-x,DMA-yy) <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) TCE is enabled. (2) Dynamic Provisioning is enabled. (3) A controller has been blocked. (4) A pair exists whose status is Paired and that is in the process of cycle copy. (5) Write access is executed to P-VOL of the pair of (4). [Cause] Firmware bug In TCE, if write is executed to an area yet to be copied in P-VOL at cycle copy being executed, data in the area is transferred to a pool before it is copied to S-VOL. For this reason, if a DRR error occurs, the firmware needs to stop the cycle copy by changing the TCE pair status to Failure. However, this changing process was omitted due to the firmware bug, resulting in the pair status not becoming Failure. <Countermeasure> The firmware has been fixed to change the TCE pair status to Failure when a DRR error occurs during cycle copy. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Apply the fixed firmware. <Web Message> Messages output when a DRR error occurs: Parity generation LA error[DRR] Parity generation LA error[DRR](CTL-x,DMA-yy) DMA error was detected(CTL-x,DMA-y) ECC write parity error(CTL-x,DMA-y) ECC generate error(CTL-x,DMA-y) ECC correction failed(CTL-x,DMA-yy)	
	4	C	A	None	VC4-0005 (Same as DF850 V25-0043)	Controller blockage may be caused by pair creation with -nocopy option in TrueCopy Extended Distance(TCE).	[Phenomena] The following phenomena occur if a pair is created with the -nocopy option in CTG where a TCE pair exists. (1) A controller is blocked in the remote array. (2) Shortly after (1), the pair status of TCE P-VOL becomes PSUE(Failure), and that of S-VOL becomes PSUS(Split) even if pair split is not performed. If the blocked controller of (1) has already recovered, the controller is also blocked that has ownership of S-VOL whose status has become PSUS(Split). <Web Message> When the controller of (1) is blocked: HJ2CC1 Microprogram error[POM] When the controller of (2) is blocked: HJ2CS5 Microprogram error[POM] <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) TCE is enabled. (2) Host write is performed to P-VOL of a TCE pair whose status is PAIR(Paired). (3) A TCE pair is created in the Consistency Group (CTG) where the pair of (2) belongs with the -nocopy option.	

							[Cause] Firmware bug When cycle transfer of TCE is completed, the internal pair status is changed. While the differential data is internally being deleted, the internal pair status can not be changed. However, if a pair exists in the same CTG whose cycle is complete after being created with the -nocopy option, the internal pair status is incorrectly changed skipping determination of whether the differential data is being deleted. This causes the process of deleting the differential data to detect incorrect changes in the internal pair status, resulting in controller blockage. (Phenomenon 1). After that, deletion and transferring to the pool of the differential data occur simultaneously, causing the management information to be incorrect. After the deletion of the differential data is complete, an error is detected in the differential data management information at the data validity check, resulting in the pair status becoming PSUE(Failure) and a controller being blocked. <Countermeasure> The firmware has been fixed to perform determination of whether the differential data is being deleted even if another pair exists whose cycle is complete in the same CTG at the completion of the cycle. [Recovery] Apply the fixed firmware. <Action in the case of the failure>			
	5	C	A	None	VC4-0009	A port may become unresponsive to the host when a host connector is blocked in the configuration where a 4 Gbps Fibre Channel (FC) interface (I/F) board is used with the transfer rate set to "Auto" in the FC settings.	[Phenomena] In the configuration where a 4 Gbps FC I/F board is used with the transfer rate set to "Auto" in the FC settings, if a host connector is blocked because of a malfunction, the automatic negotiation function is triggered every tens of microseconds in the blocked port. This may considerably increase CPU usage rates, resulting in the port that is controlled by the CPU becoming unresponsive to host I/Os. <Web Message> When a host connector is blocked: W0Pz0a Host connector alarm(PortXY) <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) A 4 Gbps FC I/F board is used. (2) All of the following conditions are met in the port of (1). - The transfer rate is set to "Auto" in the FC settings. (Default: Auto) - A cable is connected. (3) The transfer rate is set to "Auto" in an FC-connected device. (4) A host connector is blocked because of its malfunction in the port of (2). (Note 1) [Cause] Firmware bug When a port is receiving optical signals from an FC-connected device, the firmware bug causes the automatic negotiation function to negotiate without checking host connector blockage. If the blocked port continues to receive optical signals from the FC-connected device even after the host connector is blocked, the automatic negotiation function, which is unnecessary and unsuccessful, continues to be triggered periodically to increase CPU workload considerably, resulting in the CPU becoming unable to process host I/Os. <Countermeasure> The firmware has been fixed to ensure that the automatic negotiation function does not negotiate if a host connector is blocked by checking host connector blockage even if the blocked port is receiving optical signals from an FC-connected device. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Remove the blocked host connector from the FC I/F board. <Web Message> When a host connector is blocked: W0Pz0a Host connector alarm(PortXY)			
	V12.3/D, 08C3/D							4/26/2013	459	038
V12.3/D 08C3/D Base System V12.3/A 08C3/A	1	I	-	None	VC4-0018	Improved error handling in online unit addition	The online unit addition process performs the operations in a predefined order to detect connected units or HDDs. In the earlier versions, if it detects an error in the order management information, it blocks a controller. To maintain controller redundancy, the firmware has been improved to ensure that the addition process clear the management information to disable addition instead of blocking a controller if it detects an error in the order management information, which is used only at addition.			

	2	I	-	None	VC4-0022 (Same as DF850 V40-0053)	Improvement in SNMP MIB information	In SNMP Agent Support Function, the SNMP process used to respond to the SNMP manager with a fixed value of 0 as "sysUpTime" (elapsed time since the SNMP agent software started). The firmware has been improved to have the SNMP process respond with an elapsed time since the SNMP agent software started (in 10 ms increments) as "sysUpTime" if SET
	3	I	-	None	VC4-0021 (Same as DF850 V40-0021)	Improved data recovery operations with Power Saving function enabled	If [Spare Drive Operation Mode] has been set to "Variable" (Default) before data in a system drive (one of the drives in the slots of HDU-0-4 in Unit-0) is recovered, the data drive becomes a new spare drive. In the later recovery process, copy back is always performed, resulting in an increased proportion of system drives in the spare drives. If a spare drive is a system drive, data recovery takes a longer time because copy back is always performed after drive replacement. To address this, the firmware has been improved to reduce the possibility of performing copy back by implementing the following methods. 1. The data recovery process preferentially uses a non-system drive as a spare drive. 2. If a spare drive is a non-system drive at the recovery of data in a system drive, the date recovery process always performs copy back after drive replacement even if [Spare Drive Operation Mode] has been set to "Variable". (This prevents a system drive from becoming a new spare drive.) 3. If a spare drive is a system drive at the recovery of data in a system drive and [Spare Drive Operation Mode] has been set to "Variable", the data recovery process operates in the no copyback mode (*1). *1: The data recovery process assigns a data drive to a new spare drive to block the data drive after the data is recovered.
	4	I	-	None	VC4-0041	Improved E-mail Alert test mail sending function	If the user sends test mail of E-mail Alert, [E-mail Error Report] had to be set to "Disabled" if it had been set to "Enabled". To address this, the firmware has been improved to enable test mailing even if [E-mail Error Report] has been set to "Enabled".
	5	I	-	None	VC4-0025	Improvement in SnapShot(SS) restore	If SS pair LU ownership is switched because of load balancing or receiving the VMware XCOPY command during SS restore, the SS restore process suspends its operations and restarts them after the LU ownership is switched, possibly causing an unexpected Web Message "IY2000 Restore started(LU-x/y)" to be output. The firmware has been improved to ensure that the SS restore process proceeds with its operations instead of suspending them to prevent the unexpected Web Message "IY2000 Restore started (LU-x/y)" from being output.
	6	I	-	None	VC4-0012	Improved setting validation process in TrueCopy remote replication(TC) or TrueCopy Extended Distance(TCE)	In earlier versions, if a remote path of TC or TCE is created with a Remote Array ID whose first digit is incorrect being specified, the remote path creation process may block the remote path. The firmware has been improved to ensure that the remote path creation process can detect incorrect settings to indicate them by displaying the following message. DMED300007: The specified serial number is incorrect. Please specify a right serial number.
	7	I	-	None	VC4-0040	Improvement in DP management information destaging operations (*1) at DP optimization	In the earlier versions, the destaging process of the DP management information at DP optimization begins with the head of the DP information, whereas the DP optimization process monitors the completion of destaging operations beginning with the DP management information in a chunk that has been optimized. This may cause the destaging that has not started to be monitored, resulting in a destaging time-out being incorrectly detected by the DP optimization process, failing the DP optimization. The firmware has been fixed to ensure that the DP optimization process does not monitor destaging operations that has not started to detect an incorrect destaging time-out by having the destaging process perform its operations in the same order as in DP optimization. *1: The destaging process for DP management information writes
	8	I	-	None	VC4-0045(2)	HDD firmware robustness improvement during interface error	HDD firmware robustness improvement during interface error HDD Model name is below. AKH146(H2), firmware revision D02G AKH300(H2), firmware revision D02G AKH450(H1), firmware revision D02G AKH450X(H1), firmware revision D02G AKH600(H), firmware revision D02G AKH600X(H), firmware revision D02G AMF300(H), firmware revision D028 AMF600(H), firmware revision D028 For details, please refer to ECN DF800-458

	9	C	A	SD5108053,SD5109643/ DF850-33462, SD5152347/ DF800-82692	VC4-0029 (Same as DF850 V40-0069)	Controller blockage caused by a large amount of repeated packet sending when Secure communication is used in management LAN	[Phenomena] When secure communication is used for communicating with management software such as Hitachi Storage Navigator Modular 2 (HSNM2) and Hitachi Device Manager, a controller may be blocked. <Web Message> H10900 [DCTL]Fatal error of internal bus was detected[P_IRQ6] or H01H00 [DCTL]The BYTE-ENABLE error of the slave command bridge was detected(CTL-x) (x is 0 or 1) <Equipment model / Firmware version> DF800S/M/H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Access is performed by management software with secure communication (accessing the secure port of the array via HSNM2, etc.) (2) A communication packet is lost in the network and the packet is resent by the array. (3) An RST packet that is sent from management software is lost during (2). [Probability of failure] Low <Explanation> Condition of Occurrence (3) is met if only the RST packet is lost (in other cases, packets are recovered by resending by management software). [Cause] Firmware bug When the array is resending packets with Secure communication; if an RST packet (indicating communication termination) from its counterpart is lost, the resent packets are not received by the counterpart, causing the array to keep sending packets. The array initiates the termination process of the Secure communication after a timeout period of 300 seconds, but resending process in Secure communication is not complete at this time. This generates timing to trigger resending in Secure communication regardless of released internal resources, resulting in illegal reference of resources being detected to block a controller. <Countermeasure> The termination process for Secure communication has been fixed to wait for completion of resending process or TCP timeout (about 10 min.) before completing the termination process. This enables the termination process to be completed correctly even if an RST packet is not received, preventing resending process from being triggered after the internal resources are released. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Follow these steps. (1) Dummy-replace the blocked controller. (2) Change the setting to communicate without SSL for the devices that use SSL for connection. <Web Message> H10900 [DCTL]Fatal error of internal bus was detected[P_IRQ6] or H01H00 [DCTL]The BYTE-ENABLE error of the slave command bridge was detected(CTL-x)		

	10	C	A	None	VC4-0011 (Same as DF850 V25-0111)	Controller blockage caused by DP optimization of Dynamic Provisioning (HDP) in TrueCopy Extended Distance (TCE) or SnapShot (SS)	[Phenomena] In TCE or SS, DP optimization of HDP may cause controller blockage. <Web Message> HJ11D0 Microprogram error[RCH] <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.3/A(0893/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) HDP is enabled. (2) SS or TCE is enabled. (3) One of the pairs exists that meets the following conditions. - SS pair whose P-VOL is virtual LU and status PSUS(Split). - TCE pair whose P-VOL is virtual LU. - TCE pair whose S-VOL is virtual LU. (4) An optimization is performed to the DP pool where P-VOL or S-VOL of one of the pairs of (3) belongs. (5) Write access is performed to the P-VOL of one of the pairs of (3). [Probability of failure] Middle <Explanation> This problem occurs only when the addresses match for a write [Cause] Firmware bug The write process for P-VOL of a virtual LU sets to ON the write disabling attribute of the address to exclude other operations from the drive write operation. If the addresses match of P-VOL write and DP optimization page copy, the DP optimization page copy process incorrectly recognizes the condition is invalid where the write disabling attribute = ON, causing controller blockage. <Countermeasure> The firmware has been fixed to ensure that the DP optimization page copy process correctly checks the write disabling attribute to execute page copy even if the write disabling attribute is set to ON. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy-replace the blocked controller. <Web Message> HJ11D0 Microprogram error[RCH]	
	11	C	A	None	VC4-0034 (Same as DF850 V45-0051)	Controller blockage may occur when ENC is blocked.	[Phenomena] When ENC blockage is caused by its failure, a controller may also be blocked. <Web Message> W0Fzf0 ENC alarm (Unit-x, ENC-y) HJ20C7 Microprogram error[BKW] <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) One of the following is met. (1)-1 Automatic ENC firmware downloading is triggered after start of the array. (1)-2 Automatic ENC firmware downloading is triggered after firmware updating. (1)-3 Online ENC firmware downloading is performed. (1)-4 Offline ENC firmware downloading is performed. (1)-5 One of the following is caused/performed in multiple arrays. (1)-5-a HDD blockage (1)-5-b FAN blockage (1)-5-c PS blockage (1)-5-d HDD removal	

							[Cause] Firmware bug If ENC blockage occurs when the ENC controlling process is performing the operation of the condition (1) to one array, the process suspends its operations to the blocked ENC. However, if ENC blockage occurs when the ENC controlling process is performing the operation of the condition (1) to multiple arrays, the process continues its operations instead of suspending them. This causes inconsistency to be detected, resulting in controller blockage. <Countermeasure> The firmware has been fixed to ensure that the ENC controlling process suspends its operations to an ENC if it is blocked when the process is performing its operations to multiple arrays. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Follow these steps. (1) Replace the blocked ENC. (2) Dummy-replace the blocked controller. <Web Message> W0Fzf0 ENC alarm (Unit-x, ENC-y) HJ20C7 Microprogram error[BKW]
	12	C	A	None	VC4-0008 (Same as DF850 V37-0138)	Controller blockage may be caused by backend diagnosis during unit addition.	[Phenomena] Controller blockage may be caused by backend diagnosis during unit addition. <Web Message> HH920x Backend diagnosis time-out was detected[code-09] <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Unit addition is performed. (2) Backend diagnosis is triggered due to a backend path failure before the unit addition is completed. <Web message> The search for the failure part of backend route error started(Path-X,Route-Y) X:Path# Y:Route# (3) The following number of units are connected to the Path that is the target of backend diagnosis. [DF800H/DF800EH] 3 or more if the target is path#0 4 or more if the target is other than path#0 [DF800S/M/ES/EM] [Cause] Firmware bug If backend diagnosis is triggered while unit addition is performed, the addition process can not be continued. For this reason, the unit addition process does not proceed only to reach timeout before the backend diagnosis is completed. When the unit addition causes timeout, the controller is internally reset. The unit addition operation and backend diagnosis are retried from scratch after the controller is internally reset. However, the unit addition process causes timeout again because of the backend diagnosis being executed and the controller is internally reset. If a controller is internally reset two times in a day, it is blocked. <Countermeasure> The firmware has been fixed to not execute a backend diagnosis during unit addition. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Follow these steps. (1) Dummy-replace the blocked controller. (2) If a backend diagnosis is triggered after the controller recovery, replace the part indicated in the diagnosis. (3) Retry unit addition.

	13	C	B	SD5137573/ DF800-33526	VC4-0028	DP optimization may fail due to time-out in writing DP management information to a DP pool.	[Phenomena] DP optimization may fail due to time-out in writing DP management information (DP management information destaging time-out) to a DP pool. <Web Message> I6HZ00 DP Pool Optimization failed(LU-xxxx,Code-03) <Equipment model / Firmware version> DF800S/M/H, V8.0/A(0880/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Dynamic Provisioning is enabled. (2) DP pool and virtual LU are created. (3) One of the following is caused/performed. (3)-1 An HDD failure in an HDD that comprises a DP pool (primary pool) (3)-2 Firmware updating (3)-3 DP pool creation, capacity addition, reinitialization, or deletion (3)-4 Virtual LU capacity shrinkage (3)-5 One of the following during DP pool formatting (*1) - Restart of the array after planned shutdown - Reboot of the array - Restart of the array after power down (with/without cache volatilization) [Cause] Firmware bug The standard destaging process for the DP management information is triggered every 5 s to partially destage the DP management information, whereas the complete one is triggered to completely destage it if the condition (3) is met. If the condition (3) is met while the standard destaging process is being performed, the complete destaging process terminates it to completely destage the DP management information, but the flag indicating "in the process of the destaging process (normal)" remains due to the firmware bug that causes the flag to fail to be cleared. The DP optimization process checks the remaining flag indicating "in the process of the destaging process (standard)", causing a time-out of the DP management information destaging, resulting in the DP optimization failing. <Countermeasure> The firmware has been fixed to ensure that the complete destaging process for the DP management information clears the flag indicating "in the process of the destaging process (standard)" when the process is triggered. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform planned shutdown or rebooting of the array after confirming the completion of the DP pool formatting.	
	14	C	B	SD4952248/ DF800-32875	VC4-0045(1)	In Seagate SAS HDD, HDD may become unresponsive to be blocked if a transferring error occurs in the HDD when the command status is being transferred.	[Phenomena] HDD(*1) may be hung up to be unresponsive to the array firmware if a transferring error occurs in the HDD when the command status is being transferred. This results in HDD blockage. (*1): One of the following Seagate SAS HDD 1) AFK400(S) 2) AKH300(S), AKH146(S) <Web Message> W09zab HDU alarm(Unit-x,HDU-y,Type-z) I5IL00 HDU error count was over the threshold[CODE-00](Unit-x,HDU-y) or W09zab HDU alarm(Unit-x,HDU-y,Type-z) I5HZ00 HDU failure is detected[Command retry failed by PDEV time-out of HDU](Unit-x,HDU-y) <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later HDD Products/HDD Firmware Version: 1. AFK400(S), 4C0B and before 2. AKH300(S)/AKH146(S), 4C62 and before [Conditions of Occurrence]	

							[Cause] Firmware bug The Read command (A), which results in Full Cache hit, is processed by ASIC, whereas the command (B), which does not, is processed by HDD firmware. If a transferring error of the status of the command (A) occurs when the ASIC and HDD firmware process the commands simultaneously after the command (A) and (B) are received through the paths (A) and (B) respectively, the HDD firmware attempts to process the status transferring operation instead of ASIC. However, the HDD firmware bug in selecting a path where commands are processed causes a path failure because the command (A) is processed in the path (B). This causes the HDD firmware to become unresponsive, resulting in HDD blockage. <Countermeasure> The HDD firmware has been fixed to correctly select a path where commands are processed to transfer the status. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Replaced the blocked HDD. <Web Message> W09zab HDU alarm(Unit-x,HDU-y,Type-z) I5IL00 HDU error count was over the threshold[CODE-00](Unit-x,HDU-y)
	15	C	B	None	VC4-0014 (Same as DF850 V25-0107)	Pair status transition to PSUE(Failure) caused by copy operation after pair of ShadowImage (SI) or Modular Volume Migration (MVM) has become PSUE(Failure)	[Phenomena] In SI or MVM configuration, after the status of the pair in copying has become PSUE(Failure), the pair status may become PSUE(Failure) again when resync or restore is performed in SI, or migration is performed in MVM. <Web Message> IF0000 Resync failed(LU-x/y) IG0000 PSUE occurred(LU-x/y) x: P-VOL LUN, y: S-VOL LUN <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. In SI: (1) SI is enabled. (2) Four or more pairs exist whose status is COPY (Synchronizing) or RCPY (Reverse Synchronizing) in each core of a controller. (3) One or more pairs exist whose status is COPY (Synchronizing) or RCPY (Reverse Synchronizing) in another controller. (4) P-VOL or S-VOL receives write access from the host, depending on the status of the pair of (3). (COPY(Synchronizing): [Cause] Firmware bug When the pair status becomes PSUE(Failure), the copy function initializes the copy management information, but the firmware bug causes the initialization to fail if controller has been blocked before the initialization and the other controller is busy handling the maximum number of copy operations. After that, copy operation is performed to the pair whose status has become PSUE(Failure), the copy function performs copy based on the uninitialized copy management information, causing the pair status to become PSUE(Failure) at the copy completion check. <Countermeasure> The firmware is fixed to initialize the copy management information when copy or deletion is performed to the pair whose status is PSUE(Failure). [Recovery] Apply the fixed firmware. <Action in the case of the failure> Retry pair creation, resync, or restore after recovery of the blocked controller. <Web Message> IF0000 Resync failed(LU-x/y) IG0000 PSUE occurred(LU-x/y) x: P-VOL LUN, y: S-VOL LUN

	16	C	B	None	VC4-0015 (Same as DF850 V35-0052)	The pairsplit -mscas command cannot be executed or is executed in an incorrect manner in the cascade configuration of TrueCopy Extended Distance(TCE)-SnapShot(SS).	[Phenomena] In the cascade configuration of S-VOL of TCE and P-VOL of SS, the following phenomena occur if the following RAID Manager command is executed: pairsplit -mscas Phenomenon 1 The pairsplit -mscas command can not be executed regardless of the status where the SS pair can be split, causing the SS pair to become unable to be split. The following error code is displayed at this time. SKEY=0x05, ASC=0x95, ASCQ=0x76, SSB=0x9400,0x905F Phenomenon 2 The pairsplit -mscas command is executed regardless of the status where the SS pair cannot be split, causing the SS pair to be split in an incorrect manner. In this case, the pair is split in unit of pair instead of in unit of group. <Web Message> None <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. Conditions common to Phenomena (1) and (2) [Cause] Firmware bug In the process of determining whether the pairsplit -mscas command can be executed in SS pair having the MU number specified in the pairsplit -mscas command, the table having the MU number that was specified at the TCE pair operation performed last time is incorrectly referenced. As a result, if the pairsplit -mscas command is unable to be executed in the SS pair having the MU number that was specified at the TCE pair operation last time, the pairsplit -mscas command becomes unable to be executed in the SS pair having the MU number that is specified in the pairsplit -mscas command regardless of the status where it can be executed. <Countermeasure> In the process of determining whether the pairsplit -mscas command can be executed in the SS pair having the MU number specified in the pairsplit -mscas command, ensure that the table having the MU number specified in the pairsplit -mscas command is referenced. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Phenomenon 1 Split TCE pairs and split SS pairs from the remote array. Phenomenon 2	
	17	C	C	None	VC4-0027 (Same as DF850 V40-0072)	Incorrect values are displayed in Drive Pperating Rate of the drive operating information after controller SAS protocol chip is reset.	[Phenomena] Lower values are incorrectly displayed in Drive Operating Rate in the drive operating information (performance data file). If Performance Monitor is being used, the Drive Operating Rate graph shows lower values incorrectly. <Web Message> None <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Drive I/O is being processed. (2) Path failure or SAS protocol chip failure occurs and SAS protocol chip is performed Reset. (3) Immediately after (2), the drive operating information in the performance information is obtained. Alternatively, Operating Rate graph is displayed in Performance Monitor. [Probability of failure] Middle <Explanation> After a path failure or SAS protocol chip failure, if the user checks	

							[Cause] Firmware bug An incorrect value was set in the drive operating information when SAS protocol chip is reset, which is used for calculating Operating Rate. <Countermeasure> The firmware has been fixed to set correct drive operating information when SAS protocol chip is reset. [Recovery] Apply the fixed firmware. <Action in the case of the failure> [Performance data] Retry obtaining the drive operating information in the performance data. [Performance Monitor] Alternatively, retry displaying Drive Operating Rate graph in Performance Monitor. <Web Message> None			
	18	C	C	None	VC4-0023 (Same as DF850 V16-S014)	The failure MIB information will be incorrect at Spare drive blockage which is triggered at the completion of dynamic sparing operation.	[Phenomena] When the spare drive operation is executing the dynamic sparing of specification Variable (No copy back), the drive source is treated as a data drive and the drive destination as a spare drive, and after completion of dynamic sparing, the drive destination will be switched to a data drive and the drive source will be switched to spare drive. When the spare drive blockage occurs upon the completion of dynamic sparing operation, The value of MIB of the controller which detected spare drive alarm becomes the spare drive alarm, but the value of MIB of other controller becomes the data drive alarm. <Web Message> W0B724 Spare HDU alarm(Unit-x,HDU-y,Type-z) I41F00 HDU error over(Unit-x,HDU-y)[REAOV] I1GG00 HDU changed to spare(Unit-x,HDU-y) I00800 Data recovery to spare HDU(Unit-x,HDU-y) The case that this WEB message is displayed without time lag comes under these categories. <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. (1) SNMP Agent Support Function is enabled. (2) Spare Drive Operation Mode is set to Variable (No copy back) [Cause] Firmware bug If the condition (3) is met, the data recovery (dynamic sparing) process changes the type of the blocked drive from "data drive" to "spare drive" in the configuration information. After the spare drive is blocked, the SNMP process references the configuration information in each controller to update failure MIB information of each controller. In Controller (A), which blocked the spare drive, the SNMP process references the latest configuration information to update the failure MIB information, but in Controller (B), the SNMP process incorrectly references the configuration information updated before the drive type is set to spare drive, updating the failure MIB information with the data indicating the blocked drive type is data drive. This results in the failure MIB information being different between Controllers (A) and (B). <Countermeasure> The firmware has been fixed to have the failure MIB information be identical between Controllers (A) and (B) by having the SNMP process wait for the data recovery process to set the configuration information of the blocked spare drive before referencing it to update the failure MIB information. [Recovery] Apply the fixed firmware. <Action in the case of the failure> None			
	V12.3/E, 08C3/E							5/16/2013	464	-

V12.3/E 08C3/E Base System V12.3/D 08C3/D	1	C	A	SD5207512/DF800-33809,56117,82743, EUC1857853/DF850-56085, SD5211504/DF850-56112	VC4-0051	A controller may be blocked when an incorrect packet is received while write data is being received with 10 Gbps iSCSI configuration	[Phenomena] In the 10 Gbps iSCSI configuration, if the 10 Gbps iSCSI chip receives an incorrect packet from upstream (host, switch, NIC, etc.) while write data is being received, the 10 Gbps iSCSI chip firmware may incorrectly detect a failure, causing controller blockage. <Web Message> HHA0xy H-IPC hardware error was detected(CTL-x,I/F-y) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V12.1/A(08C1/A) and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. (1) A 10 Gbps iSCSI interface is used. (2) While the 10 Gbps iSCSI chip is receiving write data, it receives an incorrect packet that meets all of the following conditions: - The CRC (Checksum) of the packet is correct. - Header and Data are filled with 0s. (3) The phenomenon of (2) occurs 6 times/day. [Probability of failure] Middle <Explanation> This problem only occurs when the 10 Gbps iSCSI chip receives an incorrect packet of the condition (2). However, if the chip [Cause] 10 Gbps iSCSI chip firmware bug If the 10 Gbps iSCSI chip receives an incorrect packet of the condition (2) from upstream while it is receiving write data, it incorrectly recognizes the packet as an FCoE packet due to the incorrect iSCSI chip settings by the iSCSI chip firmware. Because the FCoE function is not used, the memory areas for the function store the internal management information of the iSCSI chip firmware. For this reason, the FCoE process of the iSCSI chip incorrectly updates the internal management information of the iSCSI chip firmware, causing the firmware to detect an iSCSI System Error. If the error occurs 6 times/day, the error count threshold is exceeded to cause controller blockage. <Countermeasure> The 10 Gbps iSCSI chip firmware has been fixed to correctly set the iSCSI chip settings to discard an incorrect packet of the condition (2), preventing an iSCSI System Error from being detected. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Follow these steps. (1) Replace the blocked controller. (2) If you can identify a device (host, switch, NIC, etc.) that sent an incorrect packet, remove it from the network or replace it.	
	2	C	A	SD5207512/DF800-56102,33817,82745	VC4-0050	A controller may be blocked during host I/O in the 10 Gbps iSCSI configuration.	[Phenomena] In the 10 Gbps iSCSI configuration, if a network failure occurs during host I/O, a controller may be blocked. <Web Message> H20100 Parity generation LA error[DRR] <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.3/A(08B3/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) A 10 Gbps iSCSI interface is used. (2) A command is suspended because of a network failure (connection disconnection) caused while write data is being received. 　(This does not apply to command suspension due to LinkDown/time-out of data transfer/receipt of reset/SoftReset of iSCSI chip.) (3) Less than 512 bytes of data are transferred to the cache memory by the iSCSI chip. 　(and the iSCSI chip firmware reports the completion of the data transfer to the array firmware indicating the size of remaining data is 0.) [Probability of failure] Middle	

							[Cause] Firmware bug The firmware performs the command suspension operation if a network failure (connection disconnection) occurs while it is receiving write data. If less than 512 bytes of data are transferred from the 10 Gbps iSCSI chip to the cache memory, the firmware generates a data validity code for the cache data by referencing the size of remaining data to be transferred reported by the iSCSI chip. However, if the iSCSI chip reports the completion of data transfer indicating the size of remaining data to be transferred is 0, the firmware fails to generate a data validity code for the cache data even if only less than 512 bytes of data have been transferred to the cache memory due to the bug in determining necessity of data validity code generation. This causes the process for checking a data validity code for cache data to detect an incorrectness of the code, resulting in controller blockage. <Countermeasure> The firmware has been fixed to always determine that data validity code generation is necessary to generate a data validity code when it suspends a command at a network failure while receiving write data. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Service the array according to the recovery procedure for "H20100 Parity generation LA error[DRR]" in the maintenance manual.			
	3	C	A	None	VC4-0052 (Same as DF850 V45-0152)	A controller may be blocked during host I/O..	[Phenomena] A controller may be blocked during host I/O. <Web Message> H20100 Parity generation LA error[DRR] <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. (1) iSCSI interface is used. (2) Two or more write commands are received simultaneously from a host. (3) Transfer of write data is suspended due to a network failure. (4) Less than 512 bytes of write data are transferred by the iSCSI chip due to (3). [Probability of failure] Middle <Explanation> This problem occurs only when the write data transfer is suspended due to a network failure. However, the iSCSI chip does not guarantee transfer in 512 bytes, resulting in the problem always occurring when the conditions are met. [Cause] Firmware bug If a segment that has dirty data in the cache generated by a write command (1) receives another write command (2) to the same segment, the management information is turned ON to indicate write areas in the cache segment. If the command is suspended, the firmware needs to calculate a write data validity code by referencing the target management information. However, because of the incorrectly cleared areas in the write area information by the completion operation for the former write command (1), which already completed the data transfer, if the latter write command (2) is suspended due to an error of transferring, the firmware fails to calculate a write data validity check code by referencing the write area information, causing the correct post process for transfer suspension to fail. This results in an inconsistency in the write data validity check code being detected to cause controller blockage. <Countermeasure> Clear the correct areas in the write area information. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Service the array according to the recovery procedure for "H20100 Parity generation LA error[DRR]" in the maintenance manual. <Web Message>			
	V12.3/F, 08C3/F							6/21/2013	465	-

V12.3/F 08C3/F Base System V12.3/E 08C3/E	1	I	-	SD5120999/DF800-33477	VC4-0063	The addition of a validity check of the management information for the settings when you change those of FC or those provided by the LUN Manager in Hitachi Storage Navigator Modular 2 (HSNM2)	When you change the settings in [Port Settings]-[FC Settings] or those provided by the LUN Manager function in HSNM2, an earlier version of the firmware blocks a controller if the management information for these settings (the number of WWNs in the Host Group Security information, etc.) is invalid. This version of firmware has been improved to check the management information for invalidity when it receives (*1) and processes (*2) the information to prevent a failure of a setting operation with an error, which leads to controller blockage. (*1) HSNM2 error message: DMEA000007: An invalid response was received from the subsystem. Confirm the subsystem status and the LAN environment, and then try again. (*2) HSNM2 error message: DMED05000C: An internal program error occurred. Wait for a while and then try again. If the problem cannot be solved, contact the maintenance personnel.	
	2	I	-	None	VC4-0068 (Same as DF850 V45-0173)	Improved unmap command reply time	The new max length of unmap command, 128MB, is supported. To use this function, enable "UNMAP Short Length Mode" in the host group/target option.	
	3	I	-	None	VC4-0058	Reduced HDD I/O delays caused by an unresponsive SAS protocol chip (SAS-CTL) (*1) (*1) SAS protocol chip (SAS-CTL): a chip that issues commands to an HDD or ENC	When a timeout occurs in an instruction for the SAS-CTL to issue commands to multiple HDDs, the backend process determines that it has become unresponsive and suspends I/O to all the HDDs before it resets the SAS-CTL to recover it from the failure. In an earlier version of the firmware, the backend process performs the same number of resets as that of the instructions timed out when the SAS-CTL becomes unresponsive. In this improved version of the firmware, the number of resets to the SAS-CTL has been reduced by resetting it only once, resulting in a reduced I/O suspension period to HDDs.	
	4	I	-	None	VC4QA003 (2)	Enhanced validity check of the DP pool management information performed when the array is started	This version of firmware has been improved to check duplication of the DP pool management information and validity of the cache memory address when the array is started and to issue the SNMP Trap (*1) and output the Web message (*2) to notify the customer/SE of the necessity of servicing the array if the checked DP pool management information is invalid. (*1) arrayRebootRequestForDPPoolInvalid and/or dpPoolInformationInvalid (*2) I6N500 DP management information may be invalid, Please reboot the array with power cycle. and/or I6N600 DP management information is invalid(DP Pool-xx)	
	5	I	-	None	VC4-0056	Improved failure handling performed when a failure to volatilize the cache memory is detected at the time of the start of the array after planned shutdown	In an earlier version of the firmware, the initial setting process blocks a controller if it recognizes that the cache memory has not been volatilized when the array is started after planned shutdown. This version of firmware has been improved to prevent controller blockage by ensuring that the initial setting process initializes the cache memory to retry initial setting.	
	6	C	A	SD5195410/DF800-33745	VC4-0057 (Same as DF850 V45-0165)	A controller may be blocked when P-VOL of a pair of TrueCopy Extended Distance (TCE) receives a write command.	[Phenomena] When P-VOL of a TCE pair receives a write command, its pair status may transition to Failure(PSUE) to cause controller blockage. <Web Message> HJ0E3O Microprogram error[CMD] or HJ0A20 Microprogram error[HSC] IB1G00 Pair status changed by the error(CTG-xx) <Equipment model / Firmware version> DF800H, V4.0/A(0840/A) and later DF800EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) TCE is enabled. (2) The local array of TCE is DF800H or DF800EH (with multi cores). (3) Two or more TCE pairs exist. (4) The pair statuses of the TCE pairs of (3) are Synchronizing(COPY) or Paired(PAIR). (5) P-VOL of the TCE pairs of (4) receives a write command. [Probability of failure] Low <Explanation>	

							[Cause] Firmware bug In a local array of TCE, Core (A) performs the cycle transfer (*) on a CTG basis when the status of a pair is PAIR or the COPY status is finished. It internally changes the pair status when the transfer is initiated and completed, and excludes this operation from I/O operations. (*)Cycle transfer: An internal copy operation periodically performed from P-VOL to S-VOL of TCE. To change pair status when one CTG includes multiple LUs that are owned by different controllers or cores, Core (A) issues a request for the initiation of Exclusive Operation (1) to Cores (B)(C)(D) in controllers. After the pair status is changed and Core (A) issues a request for the completion of Exclusive Operation (2) to Cores (B)(C)(D), if Core (B) is performing another operation, the completion of Exclusive Operatoin (2) is made to wait to be processed. If Core (B) further receives a request for the initiation of Exclusive Operation (3) by Core (C), Core (B) may process the initiation of Exclusive Operation (3), which is requested later, before it processes the completion of Exclusive Operation (2). Exclusive Operation (3) is not performed correctly, with the completion of Exclusive Operation (2) being performed after the initiation of Exclusive Operation (3). This causes an operation inconsistency to be detected due to I/O operations being processed that should be excluded, resulting in controller blockage. <Countermeasure> The firmware has been fixed to perform the completion and
	7	C	A	None	VC4QA003 (Same as DF850 V45-0146)	A controller may be blocked after restart of the array following power down without cache volatilization during DP pool deletion	[Phenomena] After power down without cache volatilization occurs while the last DP pool in the array is being deleted, if a DP pool is created and a DP-VOL receives host I/O, etc., a controller is blocked. <Web Message> HJ11H6 Microprogram error[RCH] HJ4ABG Microprogram error was detected[HDP](CTL-x) I6GU00 R/W command for the LUN is rejected due to invalid LUN process of array(LU-xxxx,yyyy) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.5/A(08B5/A) and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. (1) Dynamic Provisioning is enabled. (2) All the DP pools in the array are deleted. (3) The array is restarted after power down without cache volatilization during (2). (4) A DP pool and a DP-VOL are created after the array becomes Ready. (5) Host I/O is issued to the DP-VOL of (4). [Probability of failure] High <Explanation> This problem occurs when the conditions are met. [Cause] Firmware bug If power down without cache volatilization occurs during DP pool deletion, the process for disabling the DP management information is triggered when the array is restarted later. However, if it occurs when the last DP pool is being deleted, part of the DP management information remains incorrectly because the disabling process incorrectly determines that disabling is not required. If a DP pool is newly used later, the host I/O process detects an inconsistency in the DP management information to cause blockage of a controller because the DP management information that remains incorrectly and that for a new DP pool have been mixed. <Countermeasure> The firmware has been fixed to ensure that the DP management information disabling process correctly determines to disable all the DP management information if all the DP pools are deleted when the array is restarted after power down without cache volatilization. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform one of the following sets of steps. If backup data is available, (1) Reinitialize the DP pool.

	8	C	A	None	VC4-0066	A controller may be blocked after restart of the array after power down without cache volatilization occurs while memory reconfiguration is being processed, which is performed after Copy-on-write SnapShot (SS) or TrueCopy Extended Distance (TCE) is unlocked in the array that uses Dynamic Provisioning (HDP)	[Phenomena] After SS or TCE is unlocked in the array that uses HDP, if power down without cache volatilization occurs while the memory reconfiguration is being performed, a controller may be blocked when an operation of SS or TCE is performed or host I/O to a virtual LU is issued after the array is started. <Web Message> HJ4ABG Microprogram error was detected[HDP](CTL-x) or HJ2CXY Microprogram error[POM] <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.7/A(0897/A)and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. (1) HDP is enabled. (2) Memory reconfiguration is performed after SS/TCE is unlocked or enabled. (3) Power down without cache volatilization occurs when memory reconfiguration progress is 51%-54% or 90-94% (about 10 seconds). (4) The array is started after (3). (5) An operation of SS or TCE is performed or host I/O is issued to a virtual LU. [Probability of failure] High [Cause] Firmware bug When SS or TCE is unlocked in the array that uses HDP, the HDP initialization process changes the HDP area address in the cache memory because a differential data management area is created. However, if power down without cache volatilization occurs when this change is being processed and the array is started later, the HDP initialization process incorrectly changes back the HDP area address to what it was. This causes part of HDP areas and differential data management areas to overlap. After that, if the SS or TCE function or host I/O process is triggered, invalidity of HDP areas or differential data management areas is detected, resulting in controller blockage. <Countermeasure> The firmware has been fixed to ensure that the HDP initialization process does not incorrectly change the HDP area address when the array is started after power down without cache volatilization. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform one of the following sets of steps. If backup data is available, (1) Start the array after planned shutdown. (2) Reinitialize the DP pool. (3) Restore the data to the DP-VOL from the backup after	
	9	C	A	None	VC4-0061	A controller may be blocked when the array is started after a failure in an HDD of DMLU occurs at the time of planned shutdown	[Phenomena] After a failure occurs in an HDD of DMLU at the time of planned shutdown in the array that uses volume copy functions (*1) and you start the array without having formatted the DMLU, if a failure occurs in an HDD of DMLU when you start the array after another planned shutdown, a controller may be blocked. (*1) Volume copy functions: ShadowImage in-system replication (SI), Modular Volume Migration (MVM), TrueCopy remote replication (TC), Copy-on-write SnapShot (SS), or TrueCopy Extended Distance (TCE) <Web Message> HJ1CP0 Microprogram error[COM] <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) One or more of the following are used: SI, MVM, TC, SS, or TCE. (2) One of the following conditions is met. (2)-1 The pair status of the SI pair is COPY or PSUS. (2)-2 The pair status of the MVM pair is COPY or PSUS. (2)-3 The pair status of the TC pair is COPY, PSUS, or PSUE.	

							[Cause] Firmware bug During planned shutdown, if the amount of differential data of volume copy exceeds the predetermined amount that cannot be written to DMLU due to a failure, the DMLU access process discards the data in the DMLU to perform planned shutdown. At this time, the DMLU should be placed in the unformatted state for the user to format it for recovery, but it is not placed in the unformatted state. Discarded part of the differential data causes the invalid differential data to be written in parity areas in the DMLU. As a result, if an HDD failure occurs when the array is started later, invalid differential data is transferred from parity areas in the DMLU to the cache memory. A volume copy function detects invalidity of the differential data, resulting in controller blockage. <Countermeasure> The firmware has been fixed to ensure that the DMLU access process places the DMLU in the unformatted state when it discards differential data at planned shutdown. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Follow these steps. (1) Dummy-replace the blocked controller. (2) Format the DMLU. (3)-1 If SI, MVM, or TC pair exists, Delete the pair.
	10	C	A	None	VC4-0064 (Same as DF850 V45QA031)	Controller blockage may occur during recovery of data in an HDD that belongs to a DP pool	[Phenomena] With Dynamic Provisioning, a controller may be blocked while the data in an HDD that belongs to a DP pool is being recovered. <Web Message> HJ11H6 Microprogram error[RCH] <Equipment model / Firmware version> DF800S/M/H, V7.0/A(0870/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Dynamic Provisioning is enabled. (2) One of the data recovery operations (correction copy, spare correction, dynamic sparing, and copy back) is triggered after a failure in an HDD that belongs to a DP pool. (3) One of the following is performed to the Pool in (2). - Host I/O - A copy operation performed in one of the following: ShadowImage, SnapShot, TrueCopy remote replication, TrueCopy Extended Distance, and Modular Volume Migration. [Probability of failure] Low <Explanation> This problem occurs when the assignment of a chunk is changed [Cause] Firmware bug The data recovery process for an HDD that belongs to a DP pool determines a target chunk to obtain the LU number assigned to the chunk. It then requests exclusion of the chunk to the chunk exclusion process to prevent the LU number of the chunk from being changed with reassignment of the chunk by the operation of the condition (3). However, if the LU number of the chunk is changed by the operation of the condition (3) between the time when it is obtained and when the exclusion is performed, the chunk exclusion process fails to check the current LU number of the chunk to incorrectly terminate and the data recovery process continues its operations. This causes an inconsistency between the LU number of the chunk obtained formerly and the current one, resulting in controller blockage. <Countermeasure> The firmware has been fixed to ensure that the chunk exclusion process checks the current LU number and if it is different from an LU number obtained by the data recovery process, the chunk exclusion process does not perform exclusion and the data recovery process newly obtains an LU number. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy-replace the blocked controller.

	11	C	B	None	VC4-0038	A controller may be blocked with an Interface Board failure when planned shutdown of the array is performed	[Phenomena] If you perform planned shutdown of the array with 10 Gbps iSCSI interface, a controller may be blocked. After the planned shutdown is complete, if you start the array, Web messages are displayed indicating controller blockage. <Web Message> HH7I0x iSCSI firmware load failed (CTL-x) W3Rxyz Interface Board alarm (CTL-w, I/F-z) W01z0x CTL alarm (CTL-x) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.0/A(08B0/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) A 10 Gbps iSCSI interface is used. (2) One of the following occurs - Start of the array. - Intermittent hardware failure in a controller. - Replacement of a controller. (3) Planned shutdown is performed to the array while the 10 Gbps iSCSI protocol chip is being initialized at the time of the start of the controller in (2). (4) The array is started after (3). [Probability of failure] Low [Cause] Firmware bug Initialization of a 10 Gbps iSCSI protocol chip is triggered at the time specified in the condition (2) and the completion of the chip initialization is monitored. When planned shutdown is performed, the chip is reset to suspend host I/O. If the chip is reset by planned shutdown while the chip is being initialized, it cancels the initialization, but the firmware bug causes the initialization process to incorrectly detect time-out of the chip initialization failing to check the chip reset while it is being initialized, resulting in controller blockage with Interface Board blockage. <Countermeasure> The firmware has been fixed to ensure that the initialization process for a 10 Gbps iSCSI protocol chip checks chip reset while it is being initialized and terminates the chip initialization if it is reset to prevent incorrect detection of Interface Board blockage. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Replace the controller indicated in the Web message. <Web Message> HH7I0x iSCSI firmware load failed (CTL-x) W3Rxyz Interface Board alarm (CTL-w, I/F-z)	
	12	C	B	None	VC4-0054 (Same as DF850 V45-0131)	Planned shutdown may fail due to ENC blockage	[Phenomena] If planned shutdown is performed while ENC firmware downloading is being processed in a backend route in the array and ENC blockage occurs in the other route, the planned shutdown may fail. <Web Message> HH8W00 Backend has been down[All the routes have been blockaded] <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) ENC firmware downloading is caused by one of the following. (Only when the version of ENC firmware bundled with the array firmware is later than that of the existing ENC firmware.) - Start of the array - Replacement of an ENC - Updating of the firmware - Addition of an additional unit - Online ENC firmware downloading (2) During (1), planned shutdown of the array is caused by one of the following. (a) Turning OFF of the main switch.	

							[Cause] Firmware bug When a controller/ENC is blocked, the backend error handling process checks for a blocked part in the backend route other than that where the ENC is blocked. If planned shutdown and ENC blockage occur when the ENC is being rebooted during ENC firmware downloading, the ENC where its firmware is being downloaded is incorrectly recognized to be blocked. This causes incorrect detection of blockage of both backend routes (backend down), resulting in the planned shutdown failing. <Countermeasure> The firmware has been fixed to ensure that the backend error handling process determines that the ENC where its firmware is being downloaded is not blocked even if planned shutdown and ENC blockage occur when the ENC is being rebooted during ENC firmware downloading. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Follow these steps. (1) Identify the blocked ENC. (2) Unplug the power cable to turn off the array. (3) Plug the power cable unplugged in (2). (4) Replace the ENC identified in (1). (5) Start the array. (6) Perform planned shutdown of the array.	
	13	C	B	None	VC4-0060 (Same as DF850 V25-0114)	Load balancing may fail to improve workload balance	[Phenomena] Workload balance may not improve even if load balancing is performed. <Web Message> None <Equipment model / Firmware version> DF800S/M/H, V5.2/A(0852/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) "Load Balancing" is set to "Enable" (Default: "Enable"), which is accessible in [Performance]-[Tuning Parameter]-[System Tuning] in the tree view in Hitachi Storage Navigator Modular 2. (2) All the parameters are set to "Enabled" (Default: "Enabled") in the "Performance Measurement Items" list, which is accessible in [Performance]-[Monitoring] in the tree view in Hitachi Storage Navigator Modular 2. [Probability of failure] Medium <Explanation> This problem occurs depending on the CPU usage of controllers or cores and the number of host I/Os. [Cause] Firmware bug The load balancing function is processed in the following order. Step 1: Finds heavily loaded controller/core to determine the controller/core from which LU ownership is taken. Step 2: Finds lightly loaded controller/core to determine the controller/core to which LU ownership is given. Step 3: Select a target LU to switch LU ownership to balance the workload between controllers/cores. In Step 3 of determining a target LU to switch, workload of each LU is calculated by counting the number of host I/Os. However, the firmware bug causes the counter to be cleared with zero at the incorrect timing, producing an incorrect I/O count. This may result in workload balance not improving due to an incorrect host I/O count that is used to select a target LU to switch. <Countermeasure> The counting process of host I/Os is fixed to produce a correct host I/O count. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Disable load balancing, and then change the ownership manually if the workload balance between controllers/cores is not maintained.	

	14	C	C	None	VC4-0065 (Same as DF850 V45-B021)	Disconnection of the connection is recorded in the host log during host I/O with 10 Gbps iSCSI configuration	[Phenomena] Disconnection of the connection is recorded in the host log during host I/O with 10 Gbps iSCSI configuration. <Web Message> None <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.0/A(08B0/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) A 10 Gbps iSCSI interface is used. (2) Transfer is suspended due to the loss of an Ack packet with a network failure while write data is being transferred. (3) After the transfer is suspended in (2), the 10 Gbps iSCSI interface receives the rest of the write data. [Probability of failure] Medium <Explanation> This problem may occur when the conditions are met, but it depends on how the OS or iSCSI driver sends write the reset of the data packets after the write data transfer is suspended. [Cause] 10 Gbps iSCSI chip firmware bug The iSCSI chip firmware (FW) responds with an Ack packet after receiving write data packets. If the Ack packet is lost because of a network failure, the host resends the write data packets. In the TCP process when the iSCSI chip FW receives the resent packets, it determines whether to respond with Duplicate Ack or discard the write data packets, based on Sequence# and Ack#. However, because of the incorrect determination based on Sequence# and Ack#, it does not respond with Duplicate Ack but incorrectly discards the write data packets. Because the write data transfer is not complete, the array firmware suspends the write data transfer. If the 10 Gbps iSCSI chip FW receives the rest of the write data packets later, it recognizes the packets to be invalid to cause disconnection of the connection. <Countermeasure> The iSCSI chip FW has been fixed to make the correct determination based on Sequence# and Ack# to respond with Duplicate Ack in the TCP process when resent packets are handled. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Identify the possible failed part of the network failure to isolate it. <Web Message>	
	15	C	C	None	VC4-0044 (Same as DF850 V20-0293)	Incorrectly larger value of SPLIT-TIME is displayed on Command Control Interface(CCI).	[Phenomena] Using a pairdisplay -v smk command on CCI may display an incorrectly larger value for SPLIT-TIME. <Web Message> None <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) ShadowImage in-system replication(SI) or Copy-on-write SnapShot(SS) is enabled (2) An SI or SS pair exists on the array. (3) The SI or SS pair is split when any value in year (lower two digits)/month/date/hour/minute/second is 10 or more. (Example: Year 2010, Month 12, etc.) (4) The pairdisplay -v smk command is executed on CCI. [Probability of failure] High <Explanation> The problem can surely occur when all of the following conditions are met.	

							[Cause] Firmware bug The CCI command process displays SPLIT-TIME by converting time acquired from the chipset (RTC) to coordinated universal time (UTC). RTC should be changed to hexadecimal numbers through operations before being converted into UTC because it is represented in BCD (Binary Coded Decimal). (Example of month: '12' in BCD = '12' in decimal = '0x0C' in hexadecimal.) However, the firmware bug causes the CCI command process to directly convert RTC into UTC without changing RTC into hexadecimal numbers through operations. This results in incorrect SPLIT-TIME if any value in year (lower two digit), month, date, hour, minute, or second is 10 or more. <Countermeasure> The firmware has been fixed to ensure that CCI command process changes RTC into hexadecimal numbers through operations before converting it into UTC. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Apply the fixed firmware and execute the pairdisplay -v smk command in CCI to redisplay SPLIT-TIME. <Web Message> None			
	V12.3/G, 08C3/G							10/4/2013	477	-
V12.3/G 08C3/G Base System V12.3/F 08C3/F	1	I	-	HDS00113853/ DF800-34276	VC4-0104	Improvement of the processing for time-out failure in controller Bridge circuit	The firmware is improved so as to reset the failure to continuously use the Bridge circuit instead of immediately blocking the controller when a time-out failure occurs in the Bridge circuit in the controller. The improvement allows the controller to work continuously when a temporary time-out failure occurs in the Bridge circuit. If a permanent time-out failure occurs, the firmware blocks the controller as is conventionally done.			
	2	I	-	None	VC4-0084	Improvement for data transfer processing of SAS protocol chip	If a register of SAS protocol chip is improperly updated due to a failure of data transfer LSI of controller, the SAS protocol chip restarts the data transfer that has already been started and an HDD may be blocked. For the above, the firmware is improved to prevent the SAS protocol chip from restarting already-started data transfer and HDD from being blocked incorrectly by revoking data transfer started by the SAS protocol chip each time.			
	3	I	-	None	VC4-0095 (Same as DF850 V60-0087)	Web Message output in FC Switch connection	This allows checking for a Switch connection failure by outputting Web Messages when FLOGI fails and when a Switch connection is established after the failure.			
	4	I	-	None	VC4-0085 (Same as DF850 V60-0063)	Improved Verify command check with Windows	To support Windows Server 2012 R2, the transfer direction check logic in the Verify command is removed.			
	5	I	-	None	VC4-0070 (Same as DF850 V50-0115)	Improved the way Write Same is executed while LU ownership is changed.	Previously, when Write Same was received during LU ownership change, the array returned 07/9550 check condition. The firmware is modified as Write Same is internally retried when it is received during LU ownership change, so that Write Same will be executed without returning 07/9550 check condition.			
	6	I	-	None	VC4-0076 (Same as DF850 V50-B002)	Improved exclusion operations for Write Same and Unmap commands	The firmware is improved to notify a host of an error (sense key/sense code: 0B/C000) and to request the host to retry the command, instead of expecting the host to detect the command time-out and to retry the command as is currently done, when exclusion of Write Same command and Unmap command from other commands turns to time-out.			

	7	C	A	HDS00108782/ DF800-56295, HDS00078561/ DF800-34243	VC4-0109	Controller blockage when backend path failure occurs during HDD read processing	[Phenomena] When a backend path failure occurs during HDD read processing, a controller may be blocked. <Web Message> H0140x [DCTL]The sequencer time-out error was detected(CTL-x) or HG0100 CTL communication send time-out <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) DF800S/M/H/ES/EM (2) HDD read processing is performed by a host read I/O, a host write I/O, a pair operation of copy function, or data recovery. (3) During the HDD read processing, a backend path failure (such as CRC error and DMA error) occurs due to an ENC failure and so on. (4) Immediately after the event of (3), a path failure occurs in the same backend path of (3) again. [Probability of failure] Low [Cause] Firmware bug When a backend path failure occurs during data reading from an HDD to cache memory, firmware performs abort processing (*1) of transfer data for D-CTL (data transfer LSI). *1: Abort processing: To flush the data in DMA buffer, the firmware requests STOP to the D-CTL and then requests flag clear to initialize DMA setting information. After the STOP request, if a path failure occurs in a transfer different from the abort target transfer, due to a bug that the firmware wrongly confirms DMA buffer of the transfer different from the abort target at the flag clear request, the D-CTL detects the remaining of data in the DMA buffer whose data flushing is supposed to be complete by the STOP request, which causes a hardware failure (sequencer time-out error) leading to the controller to be blocked. When the sequencer time-out error and communication processing between controllers conflict, Web Message"HG0100 CTL communication send time-out" appears and the controller is blocked. <Countermeasure> The firmware is modified to correctly confirm DMA buffer of abort target transfer at flag clear request even when a path failure occurs in a transfer different from the abort target after STOP is requested.	
	8	C	A	HDS00147737/ DF800-34357	VC4-0096 (Same as DF850 V50-0156)	Controller blockage with Watch Dog Time Out Error or Kernel Processing Error due to security scans	[Phenomena] In the array that is receiving security scans via a network, when it is accessed with SSL (secure port connection) through WEB or HSNM2, a controller is blocked with Watch Dog Time Out Error or Kernel Processing Error. <Web Message> H90320 Watch-dog time-out or HZ0N0x Karnel Processing error (CTL-x) <Equipment model / Firmware version> DF800S/M/H, V5.0/A(0850/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) A User Management Port or Maintenance Port is successively receiving network scans. (2) The User Management Port or Maintenance Port on the same controller as (1) receives SSL access through WEB or HSNM2. [Probability of failure] Low <Explanation> The problem does not occur when the condition (1) is not met, which means the network packet sending buffer does not continue to be depleted in DF, or security scan stops for a period long	

							[Cause] Firmware bug In a state where the array is successively receiving security scans, the network packet sending buffer may continue to be depleted. In this case, the receiving process through the WEB server or HSNM2, the array waits for the buffer to be available without processing any other operation instead of responding to SSL connection requests, causing all the I/O operations in DF to become unable to be processed. This results in the diagnosis detecting a Watch Dog Time Out or Kernel Processing Error, causing controller blockage. <Countermeasure> In the process of responding to SSL connection requests, if the sending buffer is not available, the firmware is modified so that it does not wait in an operation, which enables I/O operations in DF to be processed, preventing the diagnosis from detecting a Watch Dog Time Out or Kernel Processing Error. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Stop security scans to the array and then replace the controller or reboot the array. <Web Message> H90320 Watch-dog time-out or HZ0N0x Karnel Processing error (CTL-x)
	9	C	A	None	VC4-0115	Controller blockage at failure in SATA HDD	[Phenomena] When a failure occurs in a SATA HDD, a controller may be blocked. <Web Message> H90320 Watch-dog time-out <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800H, V4.0/A(0840/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) SATA HDDs are mounted. (2) One or more of the following commands are issued to the LU of the SATA HDDs. - Read command - Write command - Verify command - Write&Verify command (3) A failure occurs in the SATA HDD that received commands of (2). [Probability of failure] Low <Explanation> [Cause] Firmware bug When a failure occurs in a SATA HDD, a failure address is returned to a command issued by the firmware. To determine what to do (blockage, reassign, etc.) to handle the failure, the firmware checks whether the failure address is within a command address range. To compare a failure address (in 512-byte blocks) and a command address range (in 520-byte blocks) at the check, the firmware converts a failure address in the one expressed in 520-byte blocks. Because the conversion is performed one by one beginning with the top of a command address range, if a failure address is far beyond the address range, the conversion takes a long time, causing a controller to be unresponsive, which results in the controller being blocked. <Countermeasure> The firmware has been fixed to convert a command address range into the one expressed in 512-byte blocks to verify whether a failure address is within the command address range. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy-replace the blocked controller. <Web Message> H90320 Watch-dog time-out

	10	C	A	None	VC4-0099 (Same as DF850 V50-0158)	Controller blockage with iSCSI Interface Board caused by broadcast of Jumbo Frame	[Phenomena] Instability such as retries of I/O to an iSCSI Port may cause controller blockage with an iSCSI Interface Board. <Web Message> HHA0xy H-IPC hardware error was detected(CTL-x,I/F-y) W3Rzhx Interface Board alarm(CTL-w,I/F-x) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.3/A(08B3/A) and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. (1) A 10Gbps iSCSI Interface Board is installed. (2) A packet is received that is not defined in the protocol and whose length is 2 K or more. (3) The broadcast of (2) is received 6 times per day. [Probability of failure] High <Explanation> This problem occurs when the conditions are met. [Cause] iSCSI firmware bug When a packet that is not defined in the protocol is broadcasted in Jumbo Frame, the iSCSI CHIP checks the data length of the packet and incorrectly recognizes it as an unexpected one, incorrectly causing a Firmware error. It resets the iSCSI CHIP to recover from the Firmware error, during which this problem occurs if a threshold is exceeded. <Countermeasure> When a packet is received that is not defined in the protocol, discard it without checking its length. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Stop broadcasting of packets that are not defined in the protocol. Replace the controller to recover from the blockage. <Web Message> HHA0xy H-IPC hardware error was detected(CTL-x,I/F-y) W3Rzhx Interface Board alarm(CTL-w,I/F-x)	
	11	C	A	None	VC4-0072	Controller blockage when firmware ver. 08C3/F is applied while phenomenon #2 of ECN DF800-465 occurs	[Phenomena] When power down without cache volatilization occurs during deletion of the last DP pool and then the DP pool is created again in a storage system with firmware of version earlier than 08C3/F, DP management information becomes invalid in some cases. (The phenomenon of #2 in ECN DF800-465) In this case, if an operation such as a host I/O runs after the firmware of version 08C3/F is applied, a controller may be blocked. <Web Message> HG0312 Resource release time-out <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V12.3/F(08C3/F) [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Firmware version earlier than 08C3/F is applied. (2) Dynamic Provisioning is enabled. (3) All DP pools in the system are deleted. (4) During the deletion of (3), power down without cache volatilization occurs, and then the system is activated again. (5) After the system becomes ready following the operation (4), DP pools and DP-VOLs are created. (6) After the operation (5), firmware version 08C3/F is applied. (7) After the operation (6), an operation such as host I/O is performed.	

							[Cause] Firmware bug In the DP monitoring processing, if an error in DP management information is detected, communication between controllers is performed and SNMP Trap is issued. However, due to a bug that the DP monitoring processing tries to perform communication between controllers after it obtains exclusion for other processing, the communication cannot be done because of the confliction with the exclusive processing. As the communication waits for release of exclusion, no response from the controller is detected and the controller is blocked. <Countermeasure> The firmware is modified to perform communication between controllers after exclusion for other processing is released. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Replace the blocked controller. <Web Message> HG0312 Resource release time-out
	12	C	A	None	VC4-0071 (Same as DF850 V50-0116)	Controller blockage caused by a failure of Memory Reconfiguration	[Phenomena] After Memory Reconfiguration fails due to drive recovery or 1-hour timeout, etc., if Memory Reconfiguration is resumed while a virtual LU is receiving host I/O, a controller is blocked. <Web Message> HJ11xx Microprogram error[RCH] or H20100 Parity generation LA error[DRR] or HF10xx Data transfer check error[xx] Note: xx can be any value. <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.5/A(08B5/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) P.P. of Dynamic Provisioning is unlocked or locked. (2) Memory Reconfiguration is performed. (3) Memory Reconfiguration fails when its progress is 50%, 79%, 80%, or 99%. (4) Memory Reconfiguration is resumed while host I/O is being processed. [Probability of failure] Medium <Explanation> This problem occurs depending on when a conflict occurs (within [Cause] Firmware bug When Memory Reconfiguration is resumed, it restarts with an incorrect area because of an incorrect state incorrectly kept by its failure handling operation, causing a special operation to be unable to be performed, failing to exclude host I/O.So,a controller is blocked. <Countermeasure> The firmware is fixed to ensure that the failure handling operation in Memory Reconfiguration does not keep an incorrect state to restart Memory Reconfiguration with a correct area. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy-replace the blocked controller. <Web Message> HJ11xx Microprogram error[RCH] or H20100 Parity generation LA error[DRR] or HF10xx Data transfer check error[xx] Note: xx can be any value.

	13	C	A	None	VC4-0074 (Same as DF850 V50-0135)	Controller blockage caused by Unmap command in TC(TrueCopy remote replication) bidirectional connection	[Phenomena] In a TC bidirectional configuration, when both P-VOLs receive the unmap command while TC pair status transition is taking place, a controller is blocked with the following message. <Web Message> HJ080H Microprogram error[FSM] <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.0/A(08B0/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) The TC PP key is enabled. (2) TC is used bidirectionally. (3) The TC pair status is Paired (PAIR)/Synchronizing (COPY). (4) Each P-VOL receives the following command: - WRITE - WRITE & VERIFY - ATS - XCOPY (copy destination) - WriteSame - UNMAP [Probability of failure] Low <Explanation> [Cause] Firmware bug Usually, command are not processed during special operations, but when TC is configured bidirectionally, the following commands are allowed to be processed. [Commands allowed to create JOB even during special operations] - VU status check (0xF1) - VU dummy data send (0xFA) - VU double-write Write (0xFD/0xFE) - VU WriteSame (0xFC) The VU dummy data send (0xFA) or VU WriteSame (0xFC) command performs PIO transfer after JOB creation. If the PIO transfer is not complete within 100 ms, the command proceeds with the next step without waiting in SLEEP. As a result, the response is sent while PIO transfer is in progress, therefore a controller is blocked. <Countermeasure> If VU dummy data send (0xFA) or VU WriteSame (0xFC) could not perform PIO transfer within 100 ms, wait in SLEEP. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy replace the blocked controller. <Web Message>		
	14	C	A	None	VC4-0081 (Same as DF850 V50QA032)	Controller blockage caused by creation of a pair of DP-VOLs in TrueCopy Extended Distance (TCE)	[Phenomena] After a TCE pair is created with DP-VOLs, if the P-VOL receives write, a controller is blocked with the following message. <Web Message> HJ0A20 Microprogram error[HSC] <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.3/A(0893/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) TCE PP key is enabled. (2) HDP PP key is enabled. (3) P-VOL and S-VOL of TCE are DP-VOLs. (4) The pair status is Synchronizing (COPY). (5) P-VOL receives write. (6) Full Capacity Mode is OFF for P-VOL. [Probability of failure] Low <Explanation> Write must be received to an unallocated page where data is being transferred from P-VOL to S-VOL during initial copy and resync copy.		

							[Cause] Firmware bug A failure of exclusion between data transfer from P-VOL to S-VOL and operations for write received to P-VOL in areas where a page is not allocated. In data transfer from P-VOL to S-VOL in areas where a page is not allocated, the firmware obtains P-VOL extent lock, requests S-VOL to release a page, and turns OFF the TCE differential. When write is received to P-VOL of TCE, it should be processed in a normal path, but it is incorrectly processed in a fast path. In a normal path, the firmware obtains P-VOL extent lock, but in a fast path, it performs the updating operation without obtaining the extent lock, causing differential operations to be performed in the same area as a result of a failure of the exclusion. In the write operation where the TCE differential that was turned ON is checked later, an inconsistency is found because it was tuned OFF <Countermeasure> Use a normal path to process write operations to areas where a page is not allocated in TCE P-VOL whose pair status is Synchronizing (COPY). [Recovery] Apply the fixed firmware. <Action in the case of the failure> Dummy replace the blocked controller. <Web Message>
	15	C	A	None	VC4-0083	Host access lost or controller 0 blockage during replacement in (Unit-0, ENC-0)	[Phenomena] After an expansion unit where spare HDDs remain specified is removed while the array is offline and the array is started, if replacement or ENC firmware downloading is performed in (Unit-0, ENC-0), one of the following phenomena (1) and (2) may occur. Phenomenon (1): Blockage of the controller 0 <Web Message> HH0A40 System HDU access error Phenomenon (2): Access lost due to failed I/O to an LU whose ownership is held by the controller 0. After that, an attempted planned shutdown fails due to PIN over. <Web Message> W3H000 PIN is over directory threshold[write will not run](DIR-0) W3G000 PIN is over directory threshold[write through](DIR-0) <Equipment model / Firmware version> DF800S/M/H, V5.0/A(0850/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] [DF800H/EH] [Cause] Firmware bug When a blocking operation is performed to an HDD in a unit that is not connected at the start of the array, incorrect internal information is set indicating the disconnection between an HDD that has the same number as Unit-0 and Unit-0, ENC-0. This information is referenced when the ENC is inserted or during ENC firmware downloading, causing a connection between ENC and HDD to be disconnected, resulting in the I/O being unable to be issued from the controller 0 to a disconnected HDD. <Countermeasure> The firmware has been fixed to prevent incorrect updating of the management information about Unit-0 when it blocks an HDD in a unit that is not connected. In addition, if Unit-0 has incorrect information at the time of online firmware updating, the fixed firmware resolves the incorrect state. [Recovery] Apply the fixed firmware. <Action in the case of the failure> (1) Perform planned shutdown of the array to restart it. (2) If (1) fails, perform one of the following: (2)-1 Unplug all the power cables from the base unit and restart the array. (2)-2 Press RSTSW on both controllers to enter the Maintenance Mode, and then restart the array. (3) If PIN remains, perform planned shutdown and restart to delete

	16	C	B	None	VC4QA004	A planned shutdown failure to be complete when it is triggered during controller replacement	[Phenomena] Phenomenon1 When planned shutdown is triggered during controller replacement, it fails to be complete. Phenomenon2 When firmware detects a thermal error during controller replacement and planned shutdown automatically works, the planned shutdown may not be complete. <Web Message> Phenomenon1: None Phenomenon2: HE0E00 Controller thermal alarm[PSOFF] <Equipment model / Firmware version> DF800S/M, V3.2/E(0832/E) and later DF800ES/EM, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) DF800S/M/ES/EM (2) A controller is replaced. (3) During controller replacement of (2); - planned shutdown of the array is performed by turning the main switch off, or - Firmware detects a thermal error (<Web Message> HE0E00 Controller thermal alarm[PSOFF]) and planned shutdown of the array is performed. [Cause] Firmware bug At planned shutdown, the system information is destaged to system drives (DHU#0 to #4 in Unit#0). The controller A (normally 0) not only performs the system information destaging but also requests the controller B (normally 1) to do the system information destaging. However, due to the firmware bug that the controller A requests controller B to destage the system information without checking whether the controller B can perform it or not, if the controller A requests the system information destaging to the controller B before the controller B performs internal initializing processing during controller replacement, the controller B clears the request of system information destaging and does not perform it. As the controller A waits for the completion of system information destaging by B, the planned shutdown cannot be complete. <Countermeasure> The firmware has been fixed so as for the controller A to determine whether the controller B can perform the system information destaging or not and to request the destaging only when the controller B is capable of doing destaging. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform the following steps.		
	17	C	B	None	VC4-0079 (Same as DF850 V50-B030)	Remote path blockage and TC pair transition to Failure(PSUE) caused by a vStorage command in TC bidirectional connection	[Phenomena] vStorage commands in TC bidirectional connection causes Command time out to block a remote path. In addition, the status of a pair whose P-VOL is receiving a vStorage command changes to Failure(PSUE). <Web Message> IB1U00 PSUE occurred[TrueCopy](LU-XXXX/YYYY) W0K000 Path alarm(Remote-NNNNNNNN,Path-Z) I90100 Command time out <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.3/A(0893/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) TC PP key is enabled. (2) TC is used bidirectionally. (3) The pair status of the pair of (2) is Paired (PAIR) or Synchronizing (COPY). (4) The above TC P-VOL receives I/O from a VMware ESX server. [Probability of failure] Low <Explanation> In a TC bidirectional configuration, a specific command must be		

							[Cause] Firmware bug In arrays where a TC bidirectional configuration is used and (1) ATS command is being processed, if (2) SVP command and (3) VU double-write write are received, a deadlock occurs. To prevent it, (2) needs to be skipped for (3) to be processed first, but (3) fails to be processed. <Countermeasure> Process (3) by skipping (2). [Recovery] Apply the fixed firmware. <Action in the case of the failure> Recover the blocked remote path and resynchronize the pair whose status has become PSUE. <Web Message> IB1U00 PSUE occurred[TrueCopy](LU-XXXX/YYYY) W0K000 Path alarm(Remote-NNNNNNNN,Path-Z) I90100 Command time out			
	V12.3/H, 08C3/H							11/11/2013	482	039
V12.3/H 08C3/H Base System V12.3/G 08C3/G	1	C	A	None	VC4-0105 (Same as DF850 V60-B012)	Host I/O delay or stop during RAID group expansion	[Phenomena] When the operations (a) or (b) are performed during RAID group (RG) expansion, host I/Os are delayed or stopped. Also the operations result in failures as follows. (a) Operation: Setting change from Hitachi Storage Navigator Moduler2 (HSNM2) Result: The setting change request fails with an error. (b) Operation: LU scan or host reboot Result: LU (device) cannot be recognized. <Web Message> None <Equipment model / Firmware version> DF800S/M/H, V5.2/A(0852/A) and later DF800ES/EM/EH, V9.0/A(0890/A) and later [Conditions of Occurrence] The problem occurs when the following condition is met. One of the following operations is performed or one of the following status changes occurs during RG expansion. <Operation on array system> - Setting change of storage system from HSNM2 <Operation on host> - LU scan from host or host activation - Use of cluster software such as Microsoft Failover Cluster and Veritas Cluster Server - Cloning in VMware ESX server [Cause] Firmware bug When a setting change request from HSNM2 or LU scan from a host is received during RG expansion, initiation of new command processing is disabled, the RG expansion processing is suspended, all of other commands in process are completed, and then the setting change from HSNM2 or the LU scan starts. However, due to the firmware bug, if the completion of other commands is delayed after the RG expansion is suspended, the suspended RG expansion resumes. As a result, because the RG expansion processing is in process, the setting change from HSNM2 and LU scan from host do not work and besides the new command processing initiation is disabled, host I/Os do not work during the time period. <Countermeasure> The firmware has been fixed to be able to immediately suspend RG expansion when a request is issued via HSNM2 to change the settings or a LU scan from a host during RG expansion. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform the following steps. (1) Turn OFF the system. (2) Turn ON the system. <Web Message>			
	V12.3/J, 08C3/J							11/29/2013	485	-

V12.3/J 08C3/J Base System V12.3/H 08C3/H	1	I	-	HDS00347983/DF800-34810, HDS00280136/DF850-34607	VC4-0122 (Same as DF850 V61-0027)	Improvement of recovery processing for media error when response delay in read command occurs due to the media error	The firmware is improved to prevent a response delay of next read command. In particular, when multiple media errors occur and response of read command is delayed at HDD read processing, if the read command is stopped by a reset from a host, the firmware memorize a sector where the media errors occur and assigns an alternative sector.
	2	I	-	None	VC4-0097 (Same as DF850 V60-0084)	Improved controller blockage handling when a hardware failure occurs at start of the array	This improvement addresses controller blockage due to timeout when the LAN initialization at start of an array is delayed by a minor correctable hardware failure.
	3	I	-	None	VC4-0093 (Same as DF850 V50-0008)	ENC firmware data validity check	If ENC firmware is corrupted, the ENC is blocked when ENC firmware downloading is performed. To prevent this, ENC firmware is checked for corruption at the time of ENC firmware downloading.
	4	I	-	None	VC4-0119 (Same as DF850 V60-B020)	Improvement for data recovery processing of SSD	In an array system with Power Saving enabled, even when Spare Drive Operation Mode is set to "Variable"(default), if specific conditions are met, Copy back processing(*1) is always performed after HDD replacement and data recovery takes time. For the above, the firmware is improved so that the Copy back processing is not performed after HDD replacement and the data recovery does not take time if the Spare Drive Operation Mode is set to "Variable" even when the specific conditions are met in the case of data recovery for SSD that is not a power saving target. *1:The firmware copies the data in spare drive back to the replaced data drive.
	5	I	-	None	VC4-0102	Improvement for control of FAN in power supply by RKAKS ENC firmware	Currently RKAKS ENC#0 firmware and ENC#1 firmware control the FAN in the power supply #0 and the FAN in the power supply #1 respectively. With the improvement to enable each of RKAKS ENC#0 firmware and ENC#1 firmware to control the FANs in the power supply #0 and #1 in the RKAKS, if one RKAKS ENC is blocked, the other RKAKS ENC firmware can prevent a rise in temperature on the blocked ENC side.
	6	I	-	None	VC4-0118	Improvement for web message to indicate initiation of Dynamic Sparing	A drive type name (Type-c) is added to the web message that indicates initiation of dynamic sparing as follows. (Before the improvement) I15A00 Dynamic sparing start (Unit-x, HDU-y) [z] (After the improvement) I6JM00 Dynamic sparing start (Unit-x, HDU-y, Type-c) [z]
	7	C	A	HDS00408867/DF800-34949	VC4-0127	Array system down due to both controller blockage, controller blockage, or drive blockage when errors occur in 2 drives in DP RAID group of RAID6 configuration	[Phenomena] When the media diagnosis function detects errors in two drives in RAID group of RAID6 configuration, one of the following failures may occur. (1) Blockage of both controller leading to array system down (2) Blockage of controller (3) Blockage of drives <Web Message> (1) Array system down due to blockage of both controllers HJ4ABS Microprogram error was detected[HDP](CTL-x) x: Controller number (2) Controller blockage HF0700 Data transfer check error[LU OWNERSHIP], or HF0106 Data transfer check error[WSEGLOCK] (3) Drive blockage IY0F00 LA error[errcode:LUN], or IY0G00 error[errcode:LBA] <Equipment model / Firmware version> DF800S/M/H, V7.0/A (0870/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Dynamic Provisioning is enabled. (2) DP RAID group in RAID6 configuration (3) The media diagnosis function of drive detects a media error in

							[Cause] Firmware bug When the media diagnosis function detects a media error in a drive in a DP RAID group of RAID6 configuration, the function locks DP management information in the error block and performs correction read. In the read processing, if the media diagnosis function detects an error in a different drive and besides the block is not the second parity, the function reserves a segment of the second parity and then retries the correction read. At the retry, due to a failure that the media diagnosis function wrongly determines that the DP management information cannot be locked, the function does not reserve a segment. Also, due to a failure of determining whether to perform the correction read or not, the function retries the correction read without reserving the segment. This results in a use of improper segment information causing a controller or a drive to be blocked. If one controller is blocked with the Web message (1), another controller is blocked and then the array system goes down. <Countermeasure> The firmware has been corrected as follows. (1) The media diagnosis processing correctly determines to lock DP management information and then reserves a segment of the second parity. (2) The media diagnosis processing correctly determines whether to perform correction read or not at a retry, and does not perform the correction read if a segment is not reserved. [Recovery]
	8	C	A	None	VC4-0110 (Same as DF850 V60-0115)	In the cascading configuration of Copy-on-write SnapShot (SS) - TrueCopy remote replication (TC) or TrueCopy Extended Distance (TCE), resynchronization of a TC or TCE pair fails to update data in S-VOL after an SS restoration failure	[Phenomena] In SS-TC or TCE cascading configuration in the local or remote array, SS restoration causes the SS pair to go into Failure with Message 1. (As expected, the cascaded SS pair becomes unable to accept Read and Write.) After all the cascaded SS pairs are deleted (as expected, cascaded P-VOL or S-VOL of TC or TCE becomes able to accept Read and Write with Message 2), resynchronization of a TC or TCE pair fails to update the data in S-VOL. <Web Message> Message 1: IB1R00 LU access was disabled[SnapShot restore failed] Message 2: IB1Q00 LU access enable[SnapShot pair canceled](LU-XXX) <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when one of the following configuration is used and either of the conditions is met. <Configuration 1> (1) All the license keys of SS, TC, and Dynamic Provisioning (DP) are enabled. (2) A cascading configuration is used with TC P-VOL - SS P-VOL or TC S-VOL - SS P-VOL. [Cause] Firmware bug In SS restoration or TCE swapping, the differential information is updated after data copy, which should be performed in the reverse order. This causes the differential information to fail to be updated even after data copy is complete when a pair status becomes Failure for some reason during SS restoration or TCE swapping, resulting in the differential data to fail to be updated in the S-VOL at TC resynchronization. <Countermeasure> In SS restoration or TCE swapping, perform data copy after differential information updating. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform the following steps. (1) Delete all the SS pairs that become unable to accept Read and Write. (2) Delete the TC (TCE) pair. (3) Create the TC (TCE) pair that was deleted. <Web Message> Message 1: IB1R00 LU access was disabled[SnapShot restore failed] Message 2: IB1Q00 LU access enable[SnapShot pair canceled](LU-XXX)

	9	C	A	None	VC4-0113 (Same as DF850 V60-0126)	During ShadowImage (SI) copy, data is not updated in S-VOL when DP Optimization is requested	[Phenomena] When DP Optimization and SI copy are processed simultaneously, SI P-VOL data is not updated to SI S-VOL. <Web Message> None <Equipment model / Firmware version> DF800S/M/H, V8.0/A (0880/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when the following conditions are met. (1) The license keys of SI and Dynamic Provisioning (DP) are enabled. (2) The SI pair consists of P-VOL and S-VOL that are DP-VOLs. (3) The copy source of the SI pair is not in the Full Capacity Mode. (4) DP Optimization (rebalancing) is performed to the copy destination of the SI pair. (5) One of the following is true. - S-VOL write (update) is performed when the copy destination is not in the Full Capacity Mode and SI pair status is PSUS(SP)(Split Pending). - The copy destination is in the Full Capacity Mode and SI pair status is COPY(Synchronizing). - In the configuration where the SS license key is enabled and SS is cascaded to the copy destination of the SI pair, the SI pair status is COPY(Synchronizing). [Cause] Firmware bug When copy destination is in the SI-SS cascading configuration, volume page of SI copy source is not allocated or temporarily allocated, and volume page of SI copy destination is already allocated, the SI copy operation performs 0 data copy. In this process, the firmware incorrectly notifies the copy destination volume of read start instead of write start to perform 0 data copy. When relocation and data updating conflict in a page, the firmware copies the data, start switching relocation, and updates the changed data before the switching is complete. The conditions for this process to be executed specifies that the target page is notified of write start. For this reason, data in a page that is notified of only read star t fails to be updated, resulting in SI P-VOL data failing to be updated to S-VOL. <Countermeasure> Ensure that write start is reported when 0 data copy is performed. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Delete the SI pair and then recreate it. <Web Message> None	
	10	C	A	None	VC4-0130	Possible array system down if media diagnosis function of drive detects media error after DP volume deletion is requested	[Phenomena] After a user request DP volume deletion, if the media diagnosis function of drive detects a media error in a block that is not yet deleted while the deleting processing is running in the background, the both controllers are blocked and the array system may go down. <Web Message> HJ12xx Microprogram error[RAD] <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Dynamic Provisioning is enabled. (2) A DP volume has "Used" capacity. (3) The DP volume of (2) is deleted. (4) While the deleting processing of (3) is running in the background, the media diagnosis function of drive detects a media error in a block that is not yet deleted. [Probability of failure] Medium <Explanation> The problem occurs when the occurrence conditions are met, but whether the problem becomes obvious or not depends on the	

							[Cause] Firmware bug When a user deletes a DP volume, the DP management information is deleted in the background. If the media diagnosis function detects a media error in a drive block corresponding to the DP management information that is not yet deleted, due to the bug, the media diagnosis function tries to convert physical LBA to logical LBA when creating an alternate sector even though the configuration information of DP volume is deleted. Because the DP VOL configuration information has been deleted, the LBA conversion fails and a controller is blocked. After that, the other controller is blocked in the same way, leading the array system to go down. <Countermeasure> The firmware has been corrected to create an alternate sector without LBA conversion when the media diagnosis function detects a media error in a drive block corresponding to the DP management information that is not yet deleted. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Turn OFF and ON the main switch, and start the system. If the phenomenon occurs immediately after the system activation and the system does not start up, install the fixed firmware offline and start the system.
	11	C	A	None	VC4-0116	Possible controller blockage due to drive blockage at data restoring Array system down in the case of another controller blockage after above event	[Phenomena] When a media error is detected in a drive during I/O processing to a normal LU or a DP volume, if one of the following failures occurs, a controller may be blocked. - After a drive is blocked, a user deletes the normal LU, RAID group, or DP pool. - After a user deletes the normal LU, RAID group, or DP pool, the drive is blocked. - At data restoring or after the completion of data restoring, the drive is blocked as a spare drive. After the above event, if the same phenomenon occurs on the other controller, both controllers are blocked and the array system goes down. <Web Message> HJ12xx Microprogram error[RAD] <Equipment model / Firmware version> DF800S/M/H, V7.0/A (0870/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) The media diagnosis function of drive detects a media error in the block A of a drive allocated to a normal LU or a DP volume. (2) The controller same as the one where the condition (1) occurs detects a media error in the block B of a drive during I/O [Cause] Firmware bug The media diagnosis function of drive checks whether a block where a media error is detected belongs to an LU or not, and creates an alternate sector if the block belongs to the LU. However, if the condition (3) is met, due to the bug that the media diagnosis function checks if the block A where the first media error occurs (the condition (1)) belongs to the LU instead of the block B, the function wrongly determines that the block B belongs to the LU even though the block B is no longer in the LU. In this case, the media diagnosis function tries to convert physical LBA to logical LBA to create an alternate sector, but the LBA conversion fails because the block B is no longer in the LU, and the controller is blocked. If the same occurs in the other controller. both controllers are blocked and the array system goes down. <Countermeasure> The firmware has been corrected to correctly check whether the block B belongs to the LU even when the condition (3) is met. [Recovery] Apply the fixed firmware. <Action in the case of the failure> If controller is blocked; Dummy replace the blocked controller. If array system goes down;

	12	C	A	None	VC4-0120 (Same as DF850 V61-0016)	Controller blockage or array system down due to media error in drive	[Phenomena] When the media diagnosis function for drive detects any media error, the controller may be blocked or the array system may go down. <Web Message> HJ11xx Microprogram error [RCH] or HJ12xx Microprogram error [RAD] or HJ34xx Microprogram error [JSD] <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V12.3/A (08C3/A) and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. (1) A normal volume is defined in the RAID group. (2) The media diagnosis function for drive in the core A (a controller in AMS2100/2300) detects a media error in a block A in a drive. (3) After (2), in the drive of (1), the media diagnosis function of the core A detects a media error in a block B that is not defined in the volume. (4) A block next to the block B, that is block C, is defined in the volume whose ownership is in the core A. Note that when one of the following conditions is met, the problem does not occur. (a) The drive of (2) is in a RAID group whose RAID level is 0. (b) For the drive of (3), data recovery is in process. [Cause] Firmware bug When the media diagnosis function detects a media error in the block B, the block C that is the next block to the block B is checked for prevention. At the preventive check, the media diagnosis function sets the type of RAID group to which the block C belongs to the management information. However, if the block B is not defined to any volume, due to the bug, the media diagnosis function does not set the RAID group type but refers the previous RAID group type that is set in the condition (2) at the preventive check. In this case, if the previous RAID group type and the RAID group type of the block C are different, the preventive check fails and the controller is blocked. When the other controller takes over the processing, the array system may go down. <Countermeasure> The firmware has been corrected so that the media diagnosis function sets the RAID group type even when the block C checked for prevention is defined in a volume. [Recovery] Apply the fixed firmware. <Action in the case of the failure> "If controller is blocked" Replace the blocked controller. "If array system goes down"	
	13	C	A	None	VC4-0125 (Same as DF850 V70-0007)	Wrongly remained TrueCopy Extended Distance (TCE) pair when remote path deletion is performed during TCE pair split	[Phenomena] After a user performs TCE pair split, if a remote path is deleted before the pair split operation is completed, the TCE pair split operation succeeds but the TCE pair that should be split may wrongly remain. The user cannot split the pair. If the above phenomenon occurs in an array system in TrueCopy Modular Distributed (TCMD) configuration, pair operations for the TCE pair created with an array system different from the aforementioned are disabled. <Web Message> None <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when the Condition1 or the Condition2 is met. [Condition1] (1) The TCE license key is effective. (2) The Dynamic Provisioning license key is effective. (3) The TCE pair is in Split (PSUS) or Failure (PSUE) status. (4) The TCE pair is split. (5) Before the TCE pair split is completed, the user deletes a remote path.	

							[Cause] Firmware bug During the TCE pair split operation, if a remote path is deleted, the pair status needs to be changed to Simplex to complete the processing, however, due to the bug, the pair split operation waits for the remote path to be connected again so that the operation cannot be completed. As a result, the TCE pair status does not change to Simplex and the pair remains wrongly. Also, uncompleted TCE pair split operation disables TCE pair operations in TCMD configuration. <Countermeasure> The firmware has been corrected to complete TCE pair split operation by changing the pair status on the local system side of the pair when the remote path is deleted. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Create the deleted path again. (so that the TCE pair is split automatically and TCMD pair operations are enabled.) <Web Message> None
	14	C	A	None	VC4-0106 (Same as DF850 V60-0129)	Subsequent unit addition may fail after a temporally failure or blockage of a controller	[Phenomena] When a temporary failure or blockage of a controller occurs, one of the following phenomena occurs. Phenomenon [1] After successful unit addition, the subsequent addition fails. In addition, a unit that is not connected is displayed in Parts Information in Web. <Web Message> I85900 Added unit failed (Unit-x) Phenomenon [2] After abnormally terminated unit addition, an HDD in the unit is blocked. Subsequent addition also fails. In addition, a unit that is not connected is displayed in Parts Information in Web. <Web Message> W09zab HDU alarm (Unit-x, HDU-y, Type-c) I30400 HDU spin up failed (Unit-x, HDU-y) I85900 Added unit failed (Unit-x) <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Cause] Firmware bug Unit addition is incorrectly retried when a temporary failure or blockage of a controller occurs immediately before online unit addition is completed successfully. The number of connected units is incremented when addition is retried, which was already incremented at the addition immediately before this addition. This causes inconsistency in the number of connected units, resulting in subsequent addition being unable to be performed correctly. The case unit addition retried is successfully, Phenomenon[1] occurs. The case unit addition retried is failed, Phenomenon[2] occurs. <Countermeasure> The firmware has been fixed to ensure that unit addition is not retried when a temporary failure or blockage of a controller occurs immediately before online unit addition is completed successfully. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform planned shutdown of the array, and then start it after connecting a unit to be added. <Web Message> I85900 Added unit failed (Unit-x)

	15	C	B	HDS00246584/DF850-82925	VC4-0124 (Same as DF850 V61-0028)	Incomplete spin-up processing when requested	[Phenomena] When a user requests drive spin-up for an array system with Power Saving enabled, the spin-up may not be completed. <Web Message> None <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.5/A (08B5/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) Power Saving is enabled. (2) A RAID group consists of 3TB or larger drives. (3) A user requests spin-down for the RAID group of (2). (4) The user requests spin-up for the RAID group of (2). (5) During the spin-up processing, one of the following operations is performed or one of the following status changes occurs. (Due to the operation or status change, the spin-up temporary stops and then restarts.) <Operation on array system> - Setting change of storage system from HSNM2 - Pair Status change of ShadowImage, Snapshot, TrueCopy remote replication, TrueCopy Extended Distance, or Modular Volume Migration - Status change by completion or failure of format - Status change with completion of drive reconstruction [Cause] Firmware bug During the spin-up processing, the spin-up processing issues READCAPACITY10 and READCAPACITY16 commands to 3TB or larger drives to obtain drive capacity. However, if the spin-up processing is stopped, due to the bug, the spin-up processing keeps the information of issuing READCAPACITY16. As a result, when obtaining drive capacity after the processing resumes, as the spin-up processing determines that the READCAPACITY16 command has been issued and does not issue the command, so that the processing cannot be completed. <Countermeasure> The firmware is corrected to initialize the information of issuing READCAPACITY16 command at resuming the spin-up processing if the spin-up processing is stopped while the READCAPACITY16 command is issued. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Turn OFF and then reboot the system. Perform planned stop and then start the system. <Web Message> None	
	16	C	B	None	VC4-0126(1) (Same as DF850 V61-0017)	Login (PLOGI) error after setting change of host group option causing new host to be unable to access array system and volumes	[Phenomena] A login (PLOGI) error occurs after host group option setting is changed and a new host may not be able to access array systems and volumes. <Web Message> None <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. (1) Fibre Channel interface is used. (2) LUN Manager license key is enabled. (3) The following operations are performed for host groups #1 and later. - Host groups to which World Wide Name (WWN) that is allowed to access is registered are deleted. - The host group setting is changed. (4) The above operations of (3) is performed 128 times in total. [Probability of failure] Medium <Explanation> Even though the phenomenon occurs when the occurrence	

							[Cause] Firmware bug When the setting of host group option is changed, the core that controls a port of the host group (HG) requests the other core to reset the HG information. However, due to the bug that the other core (latter core) reports the completion of reset with the wrong HG number, the reset of HG information cannot be completed and resource of HG information improperly remains. If the total sum of the wrongly remained resources reaches 128, that is the maximum number of login operations, new login from the host cannot be accepted and the host cannot access. <Countermeasure> The firmware has been corrected to report correct number of HG information that is reset. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Disconnect the Fibre Channel cable for the Fibre Channel interface from the port and then connect it again. <Web Message> None
	17	C	B	None	VC4-0126(2) (Same as DF850 V61-0026)	Host I/O error when Fibre Channel port whose topology is Point-to-Point is directly connected to host	[Phenomena] When the Fibre Channel port whose topology is Point-to-Point is directly connected to a host, a host I/O error occurs. <Web Message> None <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. (1) Fibre Channel interface is used. (2) LUN Manager license key is enabled. (3) The topology of Fibre Channel port is Point-to-Point. (4) The port of (3) is directly connected to a host. (5) The World Wide Name (WWN) of the host is smaller than that of the port in (3). [Probability of failure] Low <Explanation> The phenomenon occurs when the occurrence conditions are met, but the connection between a host and the Fibre Channel port whose topology is Point-to-Point is not supported. [Cause] Firmware bug In login processing, a host group (HG) number is set to login information when a PLOGI command is issued, however, due to the bug that HG number is not set correctly when the occurrence conditions are met, the login processing refers the improper HG number when receiving a SCSI command from the host and returns Check Condition whose SSB is 5/2500 (Logical Unit Not Supported) for the SCSI command, so that the host I/O ends abnormally. <Countermeasure> The firmware has been corrected to set the correct HG number in login processing when a PLOGI command is issued. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Change the topology of Fibre Channel to "Loop". <Web Message> None

	18	C	B	None	VC4-0103 (Same as DF850 V60-0080)	Incorrect HDD blockage may be caused by a failure in the backend path	[Phenomena] When a failure occurs in the backend path, an HDD may be blocked incorrectly. <Web Message> W09zab HDU alarm(Unit-x,HDU-y,Type-c) z: Chassis type, a: Drive type code, b: Drive model name code, x: Unit ID #, y: Drive #, c: Drive model name IY0000 HDU error report(Unit-x,HDU-y)[0B-4Bzz] -or- IY0000 HDU error report(Unit-x,HDU-y)[0B-47zz] x: Unit ID #, y: Drive #, z: one of the alphanumeric characters including 0-9 and A-Z <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when the following conditions are met. (1) A path failure occurs between a controller and a unit, or between units. (2) A HDU is mounted downstream (farther from the controller) from the point where the path failure occurs. (3) One of the following occurs in the same path in the route other than the one where (1) occurs. a. Removal and insertion of an ENC or HDU [Cause] Firmware bug When an HDU failure is caused by a Write command, the HDU failure threshold is incremented in the failure handling operation. The HDU failure threshold should be incremented only when an HDU failure occurs, but it is incorrectly incremented even when a path failure is caused by a Write command. For this reason, the failure threshold is incremented even in the case of a path failure, resulting in an HDU incorrectly being blocked. <Countermeasure> For a failure that is caused by a Write command, increment the HDU failure threshold only when the failure can be identified as an HDU failure. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform the following steps. (1) If a controller or ENC has been blocked, replace it. (2) Replace the blocked HDD. <Web Message> W09zab HDU alarm(Unit-x,HDU-y,Type-c) z: Chassis type, a: Drive type code, b: Drive model name code, x: Unit ID #, y: Drive #, c: Drive model name	
	19	C	B	None	VC4-0111	No transfer of audit log to syslog server	[Phenomena] Audit logs are not transferred to the syslog server. <Web Message> None <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem occurs when all the following conditions are met. (1) Audit Logging is enabled. (2) For Protocol in LAN settings, IPv6 is specified. (3) "Enable transfer to the syslog server" is set to "Enable". (4) For the Syslog server address, the IPv6 link local address (The address start with fe80) is set. (5) An operation to change settings of array system is performed from Hitachi Storage Navigator Module2 (that is an operation to be recorded in an audit log). [Probability of failure] High <Explanation> The problem always occurs when the conditions of occurrence are met.	

							[Cause] Firmware bug The processing to transfer audit logs to outside does not support IPv6 link local address. <Countermeasure> The firmware has been corrected to enable the processing that transfers audit logs to outside to adapt the IPv6 link local address. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Apply the fixed firmware. <Web Message> None
	20	C	C	HDS00367733/DF800-82977	VC4-0129	No reflection of daylight saving time setting after daylight saving time starts and ends if specific time zone of Australia is selected	[Phenomena] When one of the following time zones of Australia is selected for the Time Zone, an interlock with NTP server is set, and "Automatically adjust clock for daylight saving changes" is enabled , the daylight saving time setting is not applied to the clock after the daylight saving time starts. Also after the daylight saving time ends, the daylight saving time setting remains applied. (GMT+09:30) Adelaide (GMT+10:00) Canberra/ Melbourne/ Sydney (GMT+10:00) Hobart <Web Message> None <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem occurs when all the following conditions are met. (1) One of the following time zones of Australia is specified for the Time Zone. (GMT+09:30) Adelaide (GMT+10:00) Canberra/ Melbourne/ Sydney (GMT+10:00) Hobart (2) An interlock with NTP server is set. (3) "Automatically adjust clock for daylight saving change" is [Cause] Firmware bug In Adelaide/Canberra/ Melbourne/ Sydney/Hobart, the daylight saving time changed in 2008, and currently it starts the first Sunday in October and ends the first Sunday in March. However, the firmware does not adapt the changed daylight saving time, so that the daylight saving time setting is applied from the last Sunday in October and is released on the last Sunday in March. <Countermeasure> The firmware has been corrected to adapt the daylight saving time currently used in Adelaide/Canberra/ Melbourne/ Sydney/Hobart (changed in 2008). [Recovery] Apply the fixed firmware. <Action in the case of the failure> Apply the fixed firmware. <Web Message> None

	21	C	C	None	VC4-0112 (Same as DF850 V60-0074)	Spin down may fail in a blocked drive	[Phenomena] When a drive is blocked, it may fail to spin down. <Web Message> W09zab HDU alarm(Unit-x,HDU-y,Type-c) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V9.0/G (0890/G) and later [Conditions of Occurrence] The problem may occur when the following conditions are met. Condition A (1) A controller is inserted. (2) An HDU is blocked during (1). Condition B (1) Online firmware updating is being performed. (2) An HDU is blocked when a controller is being rebooted during (1). Condition C (1) An ENC is inserted. (2) An HDU is blocked in the unit where (1) is performed or another unit that is connected downstream to the unit. Condition D (1) Online ENC firmware updating is being performed. (2) An HDU is blocked when the ENC is being rebooted during (1). [Cause] Firmware bug When an HDU is blocked, a spin down command is issued to spin down the HDU. A spin down command is issued when: The path blockage status flags, which are managed by the firmware, are enabled in both routes; and In the management information used by the firmware, the HDU blockage status flag is enabled in an HDU to which the spin down command is issued. The path blockage status flag is disabled while the following operations are processed: controller insertion, online firmware updating, ENC insertion, and online ENC firmware updating. For this reason, the conditions that allow a spin down command to be issued may not be met depending on when an HDU is blocked, resulting in the blocked HDU being unable to spin down. <Countermeasure> The firmware has been fixed to check the blockage status of an HDU to which a spin down command is issued when disabling the path failure blockage status flag, ensuring that the path failure blockage status flag is not disabled when the blockage status flag is enabled. [Recovery] Apply the fixed firmware. <Action in the case of the failure>	
	22	C	C	None	VC4QA005	Display of Web Message with inadequate message code at blockage and recovery of drives of AVE3K and AVE3KX	[Phenomena] When any of the following messages is displayed at a blockage or recovery in a drive whose drive type is AVE3K or AVE3KX, "j" in case of AVE3K or "k" in case of AVE3KX is put in the second to the end of message code ("a" of W09$ab, for example) in the Web Message instead of "3" (expected value) for both cases. <Web Message> W09$ab HDU alarm(Unit-YY,HDU-XX,Type-cccccccc) or I007ab HDU recovered(Unit-X,HDU-Y) or I009ab Spare HDU recovered(Unit-X,HDU-X) or I5JEab Suspected failure part has been detected(Unit-XX, HDU-YY) or W0B$ab Spare HDU alarm(Unit-YY,HDU-XX,Type-cccccccc) or W0A$ab SATA HDU alarm(Unit-YY,HDU-XX,Type-cccccccc) or W0C$ab SATA Spare HDU alarm(Unit-XX,HDU-YY,Type-cccccccc) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V11.5/A (08B5/A) and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. (1) A drive whose drive name is AVE3K (3TB SATA HDD) or AVE3KX (3TB SATA HDD for RKAKX) is used. (2) In the drive of (1), a drive failure or drive recovery that results in display of Web messages shown in the phenomena occurs.	

							[Cause] Firmware bug Due to a bug to use disk drive model name code instead of disk drive type in Web Messages listed in Phenomena, wrong message codes are output in the Web Messages. <Countermeasure> The firmware has been corrected to use disk drive type to output correct message code in the Web Messages. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Apply the fixed firmware. <Web Message> W09$ab HDU alarm(Unit-YY,HDU-XX,Type-cccccccc) or I007ab HDU recovered(Unit-X,HDU-Y) or I009ab Spare HDU recovered(Unit-X,HDU-X) or I5JEab Suspected failure part has been detected(Unit-XX, HDU-YY) or W0B$ab Spare HDU alarm(Unit-YY,HDU-XX,Type-cccccccc) or W0A$ab SATA HDU alarm(Unit-YY,HDU-XX,Type-cccccccc) or W0C$ab SATA Spare HDU alarm(Unit-XX,HDU-YY,Type-cccccccc)			
	V12.3/M, 08C3/M							1/24/2014	491	-
V12.3/M 08C3/M Base System V12.3/J 08C3/J	1	I	-	None	VC4-0133	Improvement for processing of controller blockage when intermittent failure occurs in CPU peripheral part	Previously, if an intermittent failure occurs in a CPU peripheral part, the controller blockage processing collects failure information and then blocks the controller. For the processing, the firmware is improved so that the controller blockage processing blocks the controller first and then collects the failure information while the controller is blocked to promptly switch the LU ownership to another controller. With the improvement, the host can access the LU whose ownership is in the blocked controller before the switch via the other controller (with LU ownership after the switch) even when an intermittent failure occurs in a CPU peripheral part.			
	2	C	A	HDS00391207/ DF700-82970/34908	VC4-0132 (Same as DF850 V75-0010)	No response to all command on the core where AIX host command ends abnormally	[Phenomena] In a connection configuration with AIX host, if a command (command B) ends abnormally during data transfer of a read command (read command A), the core where the command ends abnormally occurs may not respond to all commands. <Web Message> None <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. (1) AIX host is connected. (2) "AIX" is set to a platform of host group (*) option for a host group (*) where the AIX host is registered. (In Additional setting of the host group (*) option, "NACA mode" is set to "Enable".) (User always sets the parameter when AIX host is connected.) (3) A volume mapped from the AIX host to the host group (*) receives the read command A and the command B. (4) During data transfer of the read command A, the command B ends abnormally. (The volume becomes ACA status for the AIX host.) (5) Before the data transfer of read command A is complete, CLEAR ACA is received from the AIX host. (6) The data transfer of read command A is completed.			

							[Cause] Firmware bug Host command control processing clears ACA status of volume when the number of incomplete commands before receiving CLEAR ACA becomes 0, and then run commands after receiving CLEAR ACA. However, if a volume becomes ACA status and CLEAR ACA is received during data transfer of read command, due to the bug that the host command control processing does not subtract the number of incomplete commands even if the read command is completed, the number of incomplete commands does not become 0 and the host command control processing does not clear the ACA status of the volume. As the host command control processing does not clear the ACA status of the volume and not run commands after receiving CLEAR ACA, commands that cannot be run are accumulated and the core that performs the processing becomes unresponsive. <Countermeasure> The firmware has been corrected to enable the host command processing to subtract the number of incomplete commands at the completion of read command and then clear ACA status of volume even when the volume becomes ACA status and CLEAR ACA is received during data transfer of read command. [Recovery] Apply the fixed firmware. <Action in the case of the failure>			
	3	C	B	HDS00323637/ DF800-56641	VC4-0131	No progress of DP optimization of DP-VOL and unable to cancel DP optimization for DP-VOL	[Phenomena] DP optimization of DP-VOL may not make any progress. (In the table of Hitachi Storage Navigator Module2 (HSNM2) tree view [Performance] - [DP optimization] - [Logical Units in the DP Pools], the status of DP-VOL in DP optimization processing remains "Optimizing (nn%) or "Suspending (nn%) and the DP optimization does not make any progress.) Also, when a user tries to cancel the DP optimization for the DP-VOL, the cancellation cannot be completed. (In the table HSNM2 tree view [Performance] - [DP optimization] - [Logical Units in the DP Pools], the status of the DP-VOL to which the DP optimization is cancelled does not change but remains "Canceling".) <Web Message> The following Web messages are not output. When the DP optimization is completed. I6HW00 DP Pool Optimization has completed[Rebalance](LU-xxxx) When the DP optimization cancellation is completed. I6HX00 DP Pool Optimization has been aborted by user(LU-xxxx) <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V12.3/D (08C3/D) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are [Cause] Firmware bug For pages that are migrated by DP optimization or those whose allocation is changed by host I/O, the firmware periodically stores DP management information of the pages on cache memory to protect the data. (Backup of DP management information) When a page to be backed up is detected by DP optimization, the backup processing of DP of DP management information determines the page as a priority page. In the following check processing to complete the DP optimization, due to a microcode bug, if the check target page is the priority page, the check processing wrongly determines that the page has been checked and does not check it. As a result, because the page to which DP optimization completion is not checked remains, the DP optimization cannot be completed. If a user cancels the DP optimization, the processing same as above takes place and the cancellation cannot be completed. <Countermeasure> The firmware has been corrected so that the check processing to complete DP optimization checks the page even when the check target page is a priority page. [Recovery] Apply the fixed firmware. <Action in the case of the failure>			
	V12.3/N, 08C3/N							3/20/2014	492	-

V12.3/N 08C3/N Base System V12.3/M 08C3/M	1	I	-	None	VC4-0137 (Same as DF850 V77-0024)	Support for display of synchronization status with NTP Server	The firmware is improved to report the Synchronization Status with NTP server (Succeeded/failed/not executed) to Hitachi Storage Navigator Modular 2(HSNM2) and enable HSNM2 to display the synchronization status. The HSNM2 window to display the Synchronization Status (GUI): [Synchronization Status] of NTP on the window opened by selecting [Settings] and then [Date & Time] in the tree view. The Synchronization Status can be displayed with the combination of firmware version 08C3/N or higher and HSNM2 version 12.63 or higher.
	2	C	A	None	VC4-0135	No response to host I/O due to no blockage of failure controller and HDD/ENC access stop at no-response failure in SAS-CTL in controller	[Phenomena] DF800S/M/ES/EM When a no-response failure occurs in a SAS protocol chip (SAS-CTL) in a controller, the failure controller is not blocked, HDD/ENC access stops on both controllers, and the following phenomena may occur. DF800H/EH When a no-response failure occurs in a SAS-CTL in a controller, the failure controller is not blocked, HDD/ENC access on both controllers for array units controlled by the SAS-CTL stops, and the following phenomena may occur. (*1) SAS-CTL #0 and #1 are mounted on a controller. The SAS-CTL #0 controls HDD/ENC in array units of backend path #0 and #1, and unit numbers of controlled array units are 0, 1, 4, 5, 8, 9... The SAS-CTL #1 controls HDD/ENC in array units of backend path #2 and #3, and unit numbers of controlled array units are 2, 3, 6, 7, 10, 11... - The both controller do not respond to host I/Os. - Data restoring (correction copy, copy back and dynamic sparing) stops. - Format of LU, virtual LU and DP pool stops. - When a planned shutdown is performed, the array system goes down. <Web Message> [Cause] Firmware bug If a no-response failure occurs in a SAS protocol chip (SAS-CTL), the processing to suspend an HDD I/O running through the SAS-CTL and the SAS-CTL reset processing work. If a permanent no-response failure occurs in the SAS-CTL, the number of SAS-CTL resets normally exceeds the threshold and the controller is blocked. However, due to a microcode bug that the HDD I/O suspending processing wrongly clears the number of SAS-CTL resets to 0 depending on the timing when a request for suspending and execution of suspending conflict each other, the number of SAS-CTL resets does not exceed the threshold even when the SAS-CTL reset works so that the failure controller is not blocked. Also, as the HDD I/O suspending processing issues a LU reset command to the HDD upon completion of SAS-CTL reset, both controllers stop issuing HDD I/Os to HDDs of array units controlled by the SAS-CTL during SAS-CTL reset processing, As a result, HDD/ENC access of the both controllers for the array units controlled by the SAS-CTL is continuously stopped, leading to phenomenon such that both controllers do not respond to host I/Os. <Countermeasure> The firmware is modified so that the HDD I/O suspending processing does not wrongly clear the number of SAS-CTL resets to 0. [Recovery] Apply the fixed firmware.

	3	C	A	None	VC4-0138 (Same as DF850 V77-0029)	Controller blockage at host connection in iSCSI configuration	[Phenomena] In iSCSI connection, a controller may be blocked when connecting to a host. <Web Message> HH7E31 Microprogram error[ILM] <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem occurs when all the following conditions are met. (1) iSCSI interface is used. (2) The total size (*1) of iSCSI Target Name that is returned to a host at login is 64 kb or larger. (3) A value larger than 64 kb is set to the max receive data segment length of OS (*2). (4) A login is performed. *1: When "Report iSCSI Full Portal List Mode" of iSCSI Target option is disabled (default): The total size of Target Name of all of iSCSI Target set to ports. When "Report iSCSI Full Portal List Mode" of iSCSI Target option is disabled (default): The total size of Target Name of all of iSCSI Target set to array system. *2: A login parameter that a host issues to an array system at login. [Cause] Firmware bug When a login is received, iSCSI login processing returns a host all of iSCSI Target Name set to iSCSI port or array system in size equal to the max receive data segment length or 64 kb at a maximum. However, due to a bug that the iSCSI login processing does not check the total size of iSCSI Target name, if the occurrence conditions are met and the total size exceeds 64 kb, exceeding login response size is detected and a controller is blocked. <Countermeasure> The firmware has been modified to check the total size of iSCSI Target Name by the iSCSI login processing so that the login response size does not exceed 64 kb. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform the following operations. (1) "Max Receive Data Segment length" setting is performed by the user on the host to a value of 64 kb or less. (2) Dummy replace the controller. <Web Message> HH7E31 Microprogram error[ILM]		
	4	C	B	None	VC4-0136 (Same as DF850 V77-0033)	Remote path blockage is not recovered automatically in TC/TCE configuration where local and remote systems are connected directly	[Phenomena] In TrueCopy remote replication (TC) or TrueCopy Extended Distance (TCE) configuration where the local system and remote system are connected directly, when a remote path is blocked due to a link down of remote path loop, the remote path may not be recovered automatically after the loop is linked up. <Web Message> I623xy The target of remote path cannot be connected(Port-xy) W0K0xy Path alarm(Remote-x,Path-y) <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all the following conditions are met. (1) Fibre Channel interface is used. (2) TC or TCE is enabled. (3) The local system and remote system are connected directly. (4) "Loop" is set for the topology of FC port property of the Fibre Channel ports that constitute the remote path. (This is the essential setting in the direct connection configuration of (3).) (5) The loop of remote path (4) is linked down and then linked up. [Probability of failure] Medium		

							[Cause] Firmware bug When a remote path is blocked and then the FC port is linked up on the local system side, the login processing performs a login to the remote system to recover the remote path. However, because of the bug that the login processing discards a request to login to the remote system if only the FC port on the local system side is linked up, the login processing does not perform a login to the remote system even if the FC port on the remote system side is linked up so that the blockage is not recovered. <Countermeasure> The firmware is modified not to discard a request to login to the remote system when only the FC port on local system side is linked up so that the login processing performs a login to the remote system after the FC port on the remote side is linked up and the remote path can be recovered. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform the following operations. (1) Remote path recovery (Hitachi Storage Navigator Module 2 (HSNM2)) GUI: Click [Recover Path x] (x = blocked path number) on the Remote Path window opened by selecting [Replication] and then [Setup] in the treeview.			
	5	C	C	None	VC4-0139	Invalid DP pool free capacity and total capacity (0) obtained when DP pool is regression state or blocked in configuration with HDI/HNAS F connected	[Phenomena] In a configuration where Hitachi Data Ingestor (HDI)/Hitachi NAS Platform F (HNAS F) is connected, if the array system information is obtained from HDI/HNAS F using SNMP Manager while a DP pool is in regression state or is blocked, values of hdpPoolFree (free capacity of the DP pool (GB)) and hdpPoolTotal (the total capacity of the DP pool (GB)) are displayed as "0". Also, if a lumaplist command is run for the DP pool, values of Free pool and Total pool are displayed as "0". Or when a user runs a command, by which Inquiry page E3 is issued, from a host (including HDI/HNAS F), the free capacity and the total capacity of the DP pool are "0". <Web Message> None <Equipment model / Firmware version> DF800S/M/H, V8.0/A (0880/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. (1) Dynamic Provisioning is enabled. (2) A HDD failure occurs and the DP-VOL status changes to Regression or Detached. (3) One of the following operations is performed. - The array system information is obtained from HDI/HNAS F using SNMP Manager in HDI/HNAS F connection configuration. [Cause] Firmware bug Due to a microcode bug that Inquiry processing unnecessarily checks DP pool status, if the DP pool is in regression state or is blocked, the Inquiry processing wrongly determines the free capacity and total capacity of DP pool in the Inquiry page E3 as invalid and sets 0 to them. <Countermeasure> The firmware is modified to set correct values to the DP pool free capacity and total capacity in the Inquiry page E3. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform the following operations. (1) According to the recovery procedure of "HDU alarm", "HDU error" and "LU alarm" indicated in Web Message, restore the data in the HDD and logical unit. (2) Retry the operation of (3) in Conditions of Occurrence. <Web Message> None			
	V12.3/R, 08C3/R							7/23/2014	501	-
V12.3/R 08C3/R Base System V12.3/N 08C3/N	1	I	-	HDS00817570/DF800-35907, HDS00075878/DF850-56309	VC4-0153 (Same as DF850 V60-B001)	Addition of "Change Response for Replication Mode" to improve the response from the array when Hardware Error or Medium Error occurs with I/Os to replication pairs.	While a host is sending I/O to a replication pair, if staging, etc. times out, it may stop accessing with Hardware Error or Medium Error returned by the array. In the "Change Response for Replication Mode", the array returns Aborted Command for a host to keep accessing. The "Change Response for Replication Mode" can be set with Hitachi Storage Navigator Modular 2 Ver.12.65 or later.			

	2	I	-	HDS00689194 DF850-35567	VC4-0141 (Same as DF850 V77-0046)	Improvement for blockage processing when PCI failure occurs in host I/O module of Fibre Channel interface	Before the improvement, when an intermittent PCI failure occurs in the Fibre Channel protocol chip mounted on host I/O module of Fibre Channel interface at system activation or firmware update, because the command processing cannot run host I/O, the blockage processing blocks a controller. For the above, the firmware is improved to enhance the PCI failure cause analysis so that the host I/O module is blocked when the above failure occurs.
	3	I	-	None	VC4-0154	Improvement for HDD firmware head diagnosis error processing	When an intermittent head diagnosis error occurs in an HDD, the HDD firmware before this improvement returns head diagnosis error (sense key/sense code: 04/44F6) for all commands received from an array system after the error and the HDD may be blocked by the array firmware. After the improvement, the HDD firmware returns the head diagnosis error only for the command that is running when the error is detected and processes other commands so that the HDD is not blocked. Model Name (Mounted HDD) - DF-F800-AKH600/AKH600X(HUS156060VLS600) - DF-F800-AKH450/AKH450X(HUS156045VLS600) - DF-F800-AKH300(HUS156030VLS600)
	4	I	-	None	VC4-0140 (Same as DF850 V77-0045)	Improvement for reduction of CPU usage when running UNMAP command	Before the improvement, when many UNMAP commands are run for a controller at an event such as deletion of large-capacity file by a user in Windows Server 2012 or VMware environment, because the command processing continues running UNMAP commands and performing page format, "Usage" of Processor information may significantly rises. For this, the firmware is improved to reduce the CPU Usage. In particular, the command processing checks the number of host I/O commands when the UNMAP Short Length Mode is enabled and the Format Priority Mode is set to Host Access or Normal, and prioritizes the host I/O commands over UNMAP command if the number of host I/O commands is large.
	5	I	-	None	VC4-0147 (Same as DF850 V60-0075)	Host login count check at online firmware updating in an array with iSCSI	During online firmware updating in an array with iSCSI, the firmware checks the host login count when firmware updating is complete in CTL0 (waits for host login up to five minutes) before starting firmware updating in CTL1.
	6	C	A	HDS01030404 DF800-83274	VC4-0161	In the event of dual bus failure between controllers, data may not be updated properly	[Phenomena] When a communication bus (Dual bus) failure occurs between controllers, if a failure of the hardware control information register (PLD register) of Controller 0 occurs at the same time, Controller 1 that should be blocked is not blocked. With this state, each controller operates assuming that "there is no need to work with the other controller because it is blocked". As a result, phenomena, such as write data received from the host is not updated, and difference management information of a replication function (ShadowImage / Copy-on-write Snapshot / TrueCopy / TrueCopy Extended Distance) is not updated, occur. Phenomena that occur due to lack of cooperation between controllers (a) When data is written to LU, data may not be updated. (b) When data is written to virtual LU, the DP pool management information of the DP pool that has the virtual LU may not be updated. (c) When data is written to a paired LU of a replication function, the difference management information of the pair may not be updated. <Web Message> - The message of a communication bus (Dual bus) failure between controllers is displayed. H07000 [DCTL]The PCI request was discarded[internal bus error][E_IRQ6](CTL-x) x: controller number [Cause] Firmware bug When a Dual bus failure occurs, both controllers detect a Dual interface error. When a controller does not have other hardware failure, it starts the processing to block the other controller. But when the processing to block the other controller runs in both of the controllers at the same time, the master controller (usually Controller 0) is not blocked to prevent array system down. The blockage processing sets the issuance information to the PLD register to issue a blockage signal to the other controller. But when a PLD register failure occurs in the master controller, the issuance information is not set, and the slave controller (usually Controller 1) is not blocked. In this case, the master controller cannot be blocked due to a firmware bug that does not check whether the issuance information is set in the PLD register. As a result, both controllers are not blocked and recognize that the other controller is blocked. Since cooperation between the controllers is lost, each controller operates independently. Consequently, firmware overwrites the latest data with the old data because it cannot keep the order of writing data between the controllers, and data may not be updated properly. Also the DP pool management information and the difference management information of a replication function are managed in both controllers, but they are updated only in the controller that receives the write command and are not updated in the other controller. <Countermeasure> The firmware is modified; - To set the issuance information to the PLD register, check

	7	C	A	None	VC4-0146 (Same as DF850 V77-0058)	When micro-program exchange is performed with iSCSI connection, response to server is delayed, and server goes down.	[Phenomena] During micro-program exchange with iSCSI connection, the virtual server (Guest OS on VMware) goes down. <Web Message> None <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] Conditions of occurrence 1 The problem may occur when all of the following conditions are met. (1) iSCSI interface board is connected (2) Online micro-program exchange (non-stop) is performed (3) Reconnection from the host takes time (The Spanning Tree function of the switch is enabled) Conditions of occurrence 2 The problem may occur when all of the following conditions are met. (1) iSCSI interface board is connected (2) Online micro-program exchange (non-stop) or micro-program exchange requiring reboot is performed (3) After exchange in Controller 0 is completed and before exchange in Controller 1 starts, I/O (PIO transfer) is received from [Cause] Cause 1 Firmware bug In online micro-program exchange (non-stop), after the reboot processing of Controller 0 is completed, the host reconnects to Controller 0. Normally the reboot processing of Controller 1 needs to be performed after the host reconnects to Controller 0. But the reconnection takes more than 30 seconds due to the Spanning Tree function in the switch, and the reboot processing of Controller 1 is performed while the reconnection is not completed. When the controller is rebooted, the host path is switched. But since reconnection of the target path is not completed, both paths are not connected, and the virtual server goes down. Cause 2 Firmware bug When micro-program transfers a command, such as Inquiry, (hereinafter referred to as "PIO transfer"), it performs the NOP-In transmission processing to prompt the host to return a response to ACK. But during micro-program exchange (after exchange in Controller 0 is completed and before exchange in Controller 1 starts), the processing is not performed due to a firmware bug, and response to ACK from the host is delayed (Delayed ACK function). As a result, processing of server I/O is delayed, and the virtual server goes down. <Countermeasure> The firmware is modified as follows. The firmware checks the number of host connections at the		
	8	C	A	None	VC4-0145	Some HDDs may be blocked by 02/0401 (Becoming ready) failure, and then access lost may occur.	[Phenomena] Some HDDs may report 02/0401 (Becoming ready) error when controller hardware failure (SAS chip failure) may occur. Some HDDs are blocked on a backend pass with the failed SAS chip, and a lot of PIN data may occur due to multiple HDD blockade, and then access lost may occur. <Web Message> IY0000 HDU error report(Unit-x,HDU-y)[02-0401] I30100 HDU error (Unit-x,HDU-y) x: Unit number, y: HDU slot number <Equipment model / Firmware version> DF-F800-AKH600/AKH600X(HUS156060VLS600)(DKR2J-K600SS), Ver. D02G and before DF-F800-AKH450/AKH450X(HUS156045VLS600)(DKR2J-K450SS), Ver. D02G and before DF-F800-AKH300(HUS156030VLS600)(DKR2J-K300SS), Ver. D02G and before DF-F800-AKH146(HUS156030VLS600)(DKR2J-K300SS), Ver. D02G and before DF800S/M/H/ES/EM/EH, V11.0/A (08B0/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) SAS chip fails with certain failure mode for which a reply sequence between the SAS chip and HDDs cannot complete (2) The specified HGST SAS HDD is mounted.		

							[Cause] HDD firmware bug HDD firmware bug which is triggered by specific failure mode of controller hardware (SAS chip). The failure mechanism is follows. A reply sequence between the SAS chip and some HDDs does not complete due to the SAS chip failure. And another controller issues RESET for the HDDs. When each HDD receives RESET, an internal timer starts. However, the HDDs cannot execute RESET due to HDD firmware bug until the reply sequence between the SAS chip and the HDDs have been completed. The HDDs execute self-reboot by the threshold over of the internal timer, and then the HDDs report 02/0401 (Becoming ready) error. <Countermeasure> The HDD firmware is modified as follows. Even if a replay sequence between SAS chip and the HDD does not complete, the HDD firmware processes RESET received from a different port. [Recovery] Apply the fixed firmware. <Action in the case of the failure> When some HDDs report 02/0401(Becoming ready) error, this problem may happen. (1) In case that PIN data occurs
	9	C	A	None	VC4-0155	Data being written turned to PIN data (*1) at array system down due to both-controller blockage when failure occurs in data transfer control LSI failure in controller	[Phenomena] During data writing, if a failure occurs in data buffer circuit of data transfer control LSI in a controller, the both controllers are blocked and the array system goes down. Also, due to the both-controller blockage, the data being written turns to PIN data. (*1) After that, when the host accesses the PIN data, as the firmware detects a DMA error and resets the host interface, host access and activation are disabled. *1: PIN data is the data that cannot be read because data assurance code becomes invalid. <Web Message> H0270x [DCTL]The master command bridge error was detected in the DUAL I/F(CTL-x) x : controller number <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) A write command is received. (2) During data writing of (1), a failure occurs in data buffer circuit for data sending (data buffer circuit) of a part for [Cause] Firmware bug When a failure occurs in the data buffer circuit in controller A, the corrupted data is transferred to cache memory in the controller B. At the time, the firmware detects the data buffer circuit failure and the controller B needs to be blocked for data preservation, but due to a bug in firmware, the data buffer circuit failure is incorrectly checked and the controller A is wrongly blocked. After that, as the controller B performs the processing using the corrupted data, the processing takes a long time and the controller B is blocked due to time-out, causing the array system to go down. Also, because of controller B blockage, retry of the corrupted data cannot work and the corrupted data turns to PIN data. <Countermeasure> The firmware is modified; (1) To correctly check the data buffer circuit, and block another controller for data preservation if a failure is detected. (2) To return an error for write command to avid the written data from turning to PIN data if a failure in the data buffer circuit is detected during data writing. (3) To check read commands to the PIN data and return a hardware error (sense key: 04) to the read command. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Take the following steps.

	10	C	A	None	VC4-0158 (Same as DF850 V60-0155/V77-0061)	I/O performance degradation in iSCSI configuration	[Phenomena] I/O performance may degrade in iSCSI configuration. <Web Message> None <Equipment model / Firmware version> iSCSI firmware Ver. 4.7.142 DF800S/M/H/ES/EM/EH, V11.3/A (08B3/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) 10Gbps iSCSI interface is used. (2) Multiple hosts are connected to iSCSI port. (3) There is a host that issues no I/O (idle status). [Probability of failure] Medium <Explanation> The performance degradation occurs in proportion to the number of connected host in idle status, but I/Os are normally issued from login hosts. [Cause] iSCSI firmware bug When any connection in idle status exists, due to a bug that I/O Queue processing unnecessary refers Queue to confirm if there is any I/O request, the I/O performance degrade due to the processing overhead. <Countermeasure> The iSCSI firmware is modified not to unnecessarily refer Queue to confirm if there is any I/O request when any connection in idle status exists. [Recovery] Apply the fixed firmware. <Action in the case of the failure> On host side, log out unused host from the array system. <Web Message> None	
	11	C	A	None	VC4-0158 (Same as DF850 V77-0072)	No response of iSCSI port to host I/O if Path MTU Discovery function on host side is used in iSCSI configuration	[Phenomena] In iSCSI configuration, if the Path MTU Discovery function on the host side is used, the iSCSI port does not return any response to host I/Os. <Web Message> None <Equipment model / Firmware version> iSCSI firmware Ver. 4.7.142 DF800S/M/H/ES/EM/EH, V11.3/A (08B3/A) and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. (1) 10Gbps iSCSI interface is used. (2) MSS (*1) is set to 560 or less in the host and network devices. For example: In case of Windows, "0" is set to registry "EnablePMTUDisocvery". The Path MTU Discovery is disabled and a packet of MSS 536bytes is sent. The default of Windows: No setting of registry "EnablePMTUDisocvery" (The Path MTU Discovery function is enabled.) (3) The host of (2) issues a read command in length of 10KB or larger. *1: MSS (Maximum Segment Size) is the maximum size of payload of packets sent at a time.	

							[Cause] iSCSI firmware bug The iSCSI firmware sends packets by dividing them for each MSS, however, when the MSS is 560bytes or less, due to a bug in calculation for dividing size of packets, a value exceeding buffer size is calculated by the iSCSI firmware. As a result, if a read command in length of 10KB or larger is received, as the iSCSI firmware tries to send the packet exceeding the buffer size, sending engine of iSCSI protocol stops and the iSCSI port becomes unresponsive to host I/Os. <Countermeasure> The iSCSI firmware is modified to correctly calculate dividing size of packet even when MSS is 560bytes or less. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Change the registry "EnablePMTUDisocvery" on the host side to "1". <Web Message> None
	12	C	A	None	VC4-0151 (Same as DF850 V60QA049 (2)/V77-0062(2))	Array system down if controller in reboot processing is blocked during firmware update and then the other controller is blocked in iSCSI configuration	[Phenomena] In iSCSI configuration, when a controller in reboot processing is blocked during firmware update, the other controller is blocked and the array system may go down. <Web Message> H0960x The PCI Express device error was detected[chipset][0xyyyyyyyy](CTL-x) x: controller number y: any value or character <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) iSCSI interface is used. (2) Online firmware update is performed. (3) During the online firmware update of (2), a failure occurs in the iSCSI protocol chip in the controller in reboot processing. (4) During the online firmware update of (2), the controller in reboot processing is blocked after (3). [Probability of failure] Medium [Cause] Firmware bug In the online firmware update, if a failure occurs in the iSCSI protocol chip in controller A while the controller A is in reboot processing, iSCSI processing of controller B resets the iSCSI protocol chip in controller A, however, due to a failure that if the controller A is blocked during time period between the chip failure and the chip reset, the iSCSI processing of controller B determines the controller that contains the reset target chip as own controller, that is the controller B, and the iSCSI processing resets the iSCSI protocol chip in controller B. As a result, a failure in the iSCSI protocol chip in controller B is detected, the controller B is blocked, and then the array system goes down. <Countermeasure> The firmware is modified so that the iSCSI processing can correctly determine the controller of chip to reset even when the controller A is blocked during time period between the chip failure and chip reset. [Recovery] Apply the fixed firmware or update the firmware for each controller one by one while stopping I/Os instead of updating in accordance with the online firmware update procedure. <Action in the case of the failure> Perform the following operations in the listed order. (1) Turn OFF the array system. (cache non-volatile)

	13	C	A	None	VC4-0157 (Same as DF850 V77QA026)	Array system down when online firmware update is retried after update fails in iSCSI configuration	[Phenomena] In iSCSI configuration, after online firmware update fails due to controller blockage or iSCSI host interface board (I/F board) blockage, if the blocked part is replaced and then the online firmware update is retried, a controller that is not in update (reboot) process is blocked and the array system may go down. <Web Message> HH7Exy Microprogram error[ILM] (x,y: any value or character) <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) iSCSI interface is used. (2) A host logs in the iSCSI port. (3) Online firmware update is performed. (4) During controller A reboot with the update, the controller A or the iSCSI I/F board of the controller A is blocked and the online firmware update is interrupted. (5) After the blocked part is replaced, the host is connected to the array system again and then the online firmware update is retried. [Probability of failure] [Cause] Firmware bug At controller A reboot associated with the online firmware update, the iSCSI processing of controller B manages the iSCSI port login information of controller A. However, there is a bug that after the blocked controller A or iSCSI I/F board is replaced, when the online firmware update is started again, the iSCSI processing of controller B does not initialize the iSCSI port login information of controller A even though the previous iSCSI port login information of controller A becomes invalid. As a result, when the iSCSI port of controller A receives login from the host during controller A reboot, if the iSCSI processing of controller B reserves the resource of login information that is not initialized, the controller is blocked due to the invalid login information resource. <Countermeasure> The firmware is modified so that the iSCSI processing of controller B initializes the iSCSI port login information of controller A at the initiation of online firmware update. [Recovery] Apply the fixed firmware. <Action to avoid the phenomenon from occurring> If a controller A blockage of iSCSI I/F board blockage occurs during online firmware update and the online firmware update is interrupted, replace the blocked part, dummy replace the controller	
	14	C	A	None	VC4-0142 (Same as DF850 V77-0049)	No response from array system for write command to TC P-VOL when host interface board failure occurs	[Phenomena] (Phenomenon 1) After host interface board (I/F board) of a port with TC remote path set is blocked, if a write command is run for a P-VOL of TC pair in PAIR status, the array system may not respond to the write command. (Phenomenon 2) After Phenomenon1 occurs, if a Hitachi Storage Navigator Modular 2 (HSNM2) operation is performed, the array system does not return any response. (Viewing web windows is enabled) For example; - Read and write commands for all LUs are disabled. - HSNM2 operations are disabled. - Planned shut down of array system disabled. <Web Message> W0K000 Path alarm(Remote-XXXXXXXX,Path-Y) W3Rxyz Interface Board alarm(CTL-Y,I/F-z) (XXXXXXXX: serial number, Y: controller number, z: slot number, x,y: any value or character) <Equipment model / Firmware version> DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The Phenomenon 1 may occur when all of the following conditions (1) to (6) are met.	

							[Cause] Firmware bug When the TC P-VOL receives a write command, the remote copy processing performs data transfer to the S-VOL using a remote path of controller that has ownership of P-VOL, however, due to a bug that if the I/F board with the remote path set is determined as "not mounted", the remote copy processing does not use an alternative path for the remote path but waits for the remote path to be recovered, the data transfer to the S-VOL cannot be complete and the array system becomes unresponsive.(Phenomenon 1) When a setting operation by HSNM2 is done while Phenomenon 1 occurs, as the setting processing waits for the completion of the write command and disables processing of all commands, the array system becomes unresponsive. <Countermeasure> The firmware is modified to perform the data transfer. In particular, the remote copy processing confirms the remote path status before starting data transfer, and uses an alternative path for the remote path to perform data transfer if the I/F board is "not mounted" status. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Replace the blocked I/F board. <Web Message>
	15	C	A	None	VC4-0150 (Same as DF850 V60QA046 /V77-0056)	I/O performance degradation resulted from wrong increase in CPU utilization after firmware upgrade	[Phenomena] In iSCSI configuration, CPU utilization reaches 80% after firmware upgrade, and the I/O performance may degrade. <Web Message> None <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) iSCSI interface is used. (2) Online firmware upgrade is performed. (3) During controller reboot in the online firmware upgrade, the iSCSI port receives a reset command from the host. [Probability of failure] Low <Explanation> Whether the problem becomes obvious or not depends on when to receive the reset command of (3). [Cause] Firmware bug There is a bug that if iSCSI processing receives a reset command from a host during controller A reboot in online firmware upgrade, the iSCSI processing reports the reset command to the controller A according to the timing when it receives the reset command even though the controller A cannot process the reset command as it is in reboot processing. After the online firmware upgrade is complete, as the iSCSI processing periodically checks the completion of reset command in the controller A, the CPU utilization to increase and the I/O performance degrades. <Countermeasure> The firmware is modified so that the iSCSI processing does not report the reset command to the controller A in reboot processing of online firmware upgrade. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform one of the following operations. (1) Dummy replacement of controller where the CPU utilization is increasing (2) Array system reboot <Web Message> None

	16	C	A	None	VC4-0152 (Same as DF850 V77-0065/V55-B007)	Controller blockage at activation in iSCSI configuration	[Phenomena] In iSCSI configuration, a controller may be blocked at controller activation (such as array system activation, controller replacement and host interface board(I/F board) replacement). <Web Message> 0181zayy H-IPC#w error [OWN_CTL] HA010x CUDG error(CTL-x) x: controller number w: port number z,a,y: any value or character <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) iSCSI interface is used. (2) One of the following events occurs and the controller is activated. - Array system activation - Array system reboot - Firmware update done for each controller one by one while stopping I/Os - Controller replacement - I/F board replacement [Cause] Firmware bug When the controller is activated, hardware diagnosis processing of iSCSI protocol chip performs data transfer diagnosis. However, due to a bug that the diagnosis processing wrongly discards the completion notice of data transfer if the completion notice of data transfer by the iSCSI protocol chip and the completion notice by the diagnosis processing conflict each other, the diagnosis processing detects a time-out of data transfer and the controller is blocked. <Countermeasure> The firmware is modified so that the hardware diagnosis processing of iSCSI protocol chip confirms all completion notices of data transfer by the iSCSI protocol chip. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Replace the I/F board of "controller number: x, port number: w". <Web Message> 0181zayy H-IPC#w error [OWN_CTL] HA010x CUDG error(CTL-x) x: controller number w: port number z,a,y: any value or character		
	17	C	B	None	VC4-0149(1) (Same as DF850 V77-0060(1))	Pair Creation/Pair Resync/Pair Split/Pair Deletion/Cycle Copy of TrueCopy Extended Distance (TCE) does not complete.	[Phenomena] The following phenomena may occur on TCE pairs. (Phenomenon 1) Pair creation or pair resync does not complete. Or Pair split or pair deletion to a pair in PAIR (Paired) (Note1) state does not complete. (Phenomenon 2) Cycle copy does not complete in PAIR (Paired) state, which means that the data on the TCE SVOL cannot be determined. (Note1) Pair states will be described in this material like below. PAIR: Description of pair states in RAID Manager (Paired): Description of pair states in Hitachi Storage Navigator Modular2 <Web Message> None <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. (1) TCE is enabled. (2) Any of the following TCE pair operations are performed. However, this is not applied for (Phenomenon 1).		

							[Cause] Firmware bug In order to verify the completion of transfer of all differential data either at the completion of data transfer for pair creation/pair resync or at the completion of a cycle copy, differential data check processing is performed from the top area of the volume (Pair A). This differential data check processing is suspended by the occurrence of an internal pair state change processing for another TCE pair (Pair B) (This differential data check processing is also suspended by Persistent Reserve Out command (Note2)). When the differential data check processing is restarted, it runs from the top area of the volume again. In a configuration where the internal pair state change processing happens periodically, the differential data processing does not complete as suspend and restart of it is repeated, which means that the pair creation/pair resync, cycle copy or pair operations involving cycle copy do not complete. (Note 2) A SCSI command which provides exclusive control of a volume between servers in HA software <Countermeasure> The firmware is modified as follows. If the differential check processing is suspended, it records an area in volume where the processing is stopped, and starts from the area when the suspended processing resumes. [Recovery] Apply the fixed firmware.
	18	C	B	None	VC4-0149(2) (Same as DF850 V77-0060(2))	Pair Creation/Pair Resync of TrueCopy(TC) does not complete.	[Phenomena] When the array receives Persistent Reserve Out commands (Note1) periodically, even if TC pair creation or pair resync is performed, the pair state does not change from COPY (Synchronizing) (Note2) to PAIR (Paired). (Note1) A SCSI command which provides exclusive control of a volume between servers in HA software (Note2) Pair states will be described in this material like below. COPY: Description of pair states in RAID Manager (Synchronizing): Description of pair states in Hitachi Storage Navigator Modular2 <Web Message> None <Equipment model / Firmware version> DF800S/M, V3.2/E (0832/E) and later DF800H, V4.0/A (0840/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. (1) TC is enabled (2) Any of the following TC pair operations are performed and the status of TC pair is COPY(Synchronizing). - Pair creation (Initial Copy). - Pair resync (3) A TC pair exists that meets any of the following volume size [Cause] Firmware bug In order to verify the completion of transfer of all data at the completion of data transfer for pair creation/pair resync, differential data check processing is performed from the top area of the volume (A). This differential data check processing is suspended by receiving the Persistent Reserve Out command (B). When the differential data check processing is restarted, it runs from the top area of the volume again (C). If the Persistent Reserve Out commands are received periodically, the differential data processing does not complete as suspend and restart of it is repeated, which means that the pair state does not change to PAIR (Paired). <Countermeasure> The firmware is modified as follows. If the differential check processing is suspended, it records an area in volume where the processing is stopped, and starts from the area when the suspended processing resumes. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Increase the interval where the host sends Persistent Reserve Out commands to the storage to increase the value of X so that Condition (3) will not be met. Set more than 64 [s] to the interval to prevent the phenomenon from occurring regardless of the TC PVOL size.

	19	C	B	None	VC4-0144 (Same as DF850 V60QA045 /V77-0054)	Firmware update uncompleted if performed after firmware downgrade	[Phenomena] When firmware upgrade is performed after the firmware is downgraded, the upgrade operation may not be complete. <Web Message> None <Equipment model / Firmware version> DF800S/M/H/ES/EM/EH, V12.3/F (08C3/F) and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. (1) The firmware of array system is downgraded from Ver. 08C3/F or later to earlier than Ver. 08C3/F. (2) In the firmware downgrade of (1), exclusive I/O processing (*1) runs per LU in the controller #1 while the firmware of controller #0 is downgraded but the firmware of controller #1 is not yet downgraded. (3) After (2), the firmware of controller #1 is downgraded. (4) After (3), the firmware is updated to Ver. 08C3/F or later. *1: The exclusive I/O processing per LU runs at the time when; - Load balance works, - An Xcopy command (*2) is received, or - An ATS command (*3) is received etc. *2: An XCOPY command is executed when one of the following operations, etc. is performed on the VMware ESX server, etc. - Cloning [Cause] Firmware bug When the occurrence conditions (1) and (2) are met, due to a bug that the exclusive I/O processing of occurrence condition (2) does not initialize a reservation flag for exclusive resource, the exclusive I/O processing that works at the controller reboot of occurrence condition (4) cannot reserve the exclusive resource, which disables the firmware upgrade to be completed. <Countermeasure> The firmware is modified as follows. The exclusive I/O processing checks whether exclusive lock is in process or not in advance. If the exclusive lock is not yet performed, the reservation flag for exclusive resource is initialized and then the exclusive I/O processing so as to enable the firmware upgrade to be complete. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform planned shutdown for the array system, and start it again. <Web Message> None			
	V12.3/S, 08C3/S							8/8/2014	510	040
V12.3/S 08C3/S Base System V12.3/R 08C3/R	1	I	-	None	VC4-0162	Reduction in HDD blockage by cleaning with full track seek	The HDD firmware is improved. With the improvement, the HDD firmware periodically performs full track seek that can move the magnetic head widely so that grease adhered to the disk surface and the magnetic head can be removed, reducing HDD blockage caused by head diagnosis errors (sense key/sense code: 04/44F6) and uncorrectable errors (sense key/sense code: 03/1100) due to the grease. HDD Model name is below. AKH146(H2), HDD firmware version D02P AKH300(H2), HDD firmware version D02P AKH450(H1)/AKH450X(H1), HDD firmware version D02P AKH600(H)/AKH600X(H), HDD firmware version D02P			
	V12.3/U, 08C3/U							8/29/2014	512	-
V12.3/U 08C3/U Base System V12.3/S 08C3/S	1	I	-	None	VC4-0164	Drive Firmware has HDD idle function parameter optimization.	Drive Firmware has HDD idle function parameter optimization. HDD Model name is below. AKH146(S1), HDD firmware version 4C60 and later AKH300(S1), HDD firmware version 4C60 and later AKH450(S), HDD firmware version 4C60 and later AKH300(S2), HDD firmware version 5C5B and later AKH450(S1), HDD firmware version 5C5B and later AKH450X(S1), HDD firmware version 5C5B and later AKH600(S), HDD firmware version 5C5B and later AKH600X(S), HDD firmware version 5C5B and later ANH600(S), HDD firmware version 5CE8 and later ANH600X(S), HDD firmware version 5CE8 and later			

	2	C	A	HDS01161627 DF800-36553	VC3-0003 (Same as DF850 V77-0087)	Controller blockage at HDU link failure in RAID group without HDD redundancy	[Phenomena] When an HDU link failure occurs in a RAID group that does not have HDD redundancy, a controller may be blocked. <Web Message> HG0312 Resource release time-out I30100 HDU error(Unit-yy,HDU-zz) yy:unit number, zz:HDU number <Equipment model / Firmware version> DF800S/M/H, V5.0/A (0850/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem may occur when all of the following conditions are met. (1) 2 HDDs (3 HDDs in RAID6 configuration) are blocked in a RAID group. (2) In HDDs in use in the RAID group of (1), a link failure occurs frequently. [Probability of failure] Low <Explanation> The probability is low because whether the phenomenon becomes obvious or not depends on the timing when the check processing (several msec) of auto ENC firmware replacement in back-end diagnosis that runs at link failure and the periodical check [Cause] Firmware bug When an HDD link failure occurs, the back-end diagnosis works and it performs the check processing of auto ENC firmware replacement. Meanwhile, the periodical check processing of auto ENC firmware replacement runs on one-second cycle. If the two check processings conflict, both processings wait for the completion of the other processing on each other and the both of them do not make progress, which eventually turns to time-out and the controller is blocked. <Countermeasure> The firmware is modified as follows. When the check processing of auto ENC firmware replacement by back-end diagnosis and the periodical check processing of auto ENC firmware replacement conflict each other, the former check processing runs first and then the latter runs. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Replace the blocked controller. <Web Message> HG0312 Resource release time-out I30100 HDU error(Unit-yy,HDU-zz) yy:unit number, zz:HDU number	
	3	C	B	HDS01091411 DF800-57187	VC4-0165	DP optimization failed wrongly	[Phenomena] When a user performs DP optimization, the DP optimization may turn to time-out and fail. <Web Message> I6HZ00 DP Pool Optimization failed(LU-X,Code-03) X: LU number <Equipment model / Firmware version> DF800S/M/H, V8.0(0880/A) and later DF800ES/EM/EH, V9.0(0890/A) and later [Conditions of Occurrence] The problem may occur when all the following conditions (1) to (4) are met if the firmware version is earlier than 08C1/A. The problem may occur when the following conditions (1) to (3) are met if the firmware version is 08C1/A or later. (1) Dynamic Provisioning is enabled. (2) Multiple DP RAID groups are created in a DP pool or multiple DP pools are created. (3) A user performs DP optimization for a DP volume in the DP pool. (4) After (3), the following operations or failures is performed or occurs. (4-1) The user deletes a DP pool different from that of (3). (4-2) An HDD constituting the DP pool is blocked. (4-3) In the DP RAID group that is in regression status before the operation (3), a failure occurs in an HDD in use. (4-4) A controller is blocked.	

							[Cause] Firmware bug The DP optimization processing de-stages the DP management information to an HDD and a core that has the ownership of alternative LU of primary pool monitors time-out. However, due to a bug that the DP optimization processing calculates the time required for de-staging wrongly if the core with the ownership of alternative LU of primary pool is switched by the condition (4) and there is 30-minute or longer difference in the time kept inside controller between two controllers, a time-out is detected for the de-staging and the DP optimization fails. <Countermeasure> The firmware is modified to correctly calculate the time required for de-staging of DP management information even when the core that has the ownership of alternative LU of primary pool is switched. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Perform the following operations. (1) Stop the DP optimization that ends abnormally. (2) Perform planned stop for the array system and then start it again. (3) Retry the DP optimization. <Web Message>
	4	C	C	None	VC4-0166 (Same as DF850 V77-0053)	Wrongly reported message indicating "capacity of created DP volume exceeds alert threshold" at DP-VOL creation	[Phenomena] When a DP-VOL is created, a Web message indicating "the capacity of created DP-VOL exceeds the alert threshold for over provisioning." may be reported wrongly. In this case, if [Yes] is specified for [Report] for [Over provisioning] and the E-Mail alert function and SNMP Agent Support function are used, mails and SNMP TRAP to report that "the capacity of created DP-VOL exceeds the alert threshold for over provisioning." are issued. <Web Message> I6GK00 Over Provisioning Ratio Forewarning(Pool-x) x:pool number <Equipment model / Firmware version> DF800S/M/H, V7.0/A (0870/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. (1) Dynamic Provisioning is enabled. (2) The value of "the total DP pool capacity multiplied by the alert threshold for over provisioning" is greater than 137438953600. (When the alert threshold for over provisioning is 100% as default, if the total DP pool capacity is 1.28PB or greater, condition (2) is met.) (3) A user creates a DP-VOL. [Probability of failure] [Cause] Firmware bug Whether the capacity of created DP-VOL exceed the capacity threshold or not is checked by calculating the capacity threshold from the total pool capacity and the alert threshold for over provisioning. However, the capacity threshold is smaller than what expected due to a bug in the calculation method for the capacity threshold. As a result, even when a DP-VOL whose capacity does not exceed the capacity threshold is created, the check processing wrongly determines that "the capacity of created DP-VOL exceeds the alert threshold" and reports related Web messages, mails, and SNMP TRAP. <Countermeasure> The firmware is modified to correctly calculate the capacity threshold from the total pool capacity and the alert threshold for over provisioning. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Change the value of alert threshold for over provisioning to be a smaller one so that the condition that the total DP pool capacity multiplied by the alert threshold for over provisioning is greater than 137438953600 is not met, or reduce the total DP pool capacity.

	5	C	C	None	VC4-0167 (Same as DF850 V77-0082)	Inadequate report of warning, "The DP volume capacity of the DP pool exceeded the Over Provisioning Ratio Forewarning threshold value"	[Phenomena] If the difference in value between Warning Alert threshold and the Limit Alert threshold of Over Provisioning Threshold is less than 5%, a warning message; "The DP volume capacity of the DP pool exceeded the Over Provisioning Ratio Forewarning threshold value." is reported to users even though the DP pool capacity does not exceed the Warning Alert threshold. In this case, if [Yes] is specified for [Report] for [Over provisioning] and the E-Mail alert function and SNMP Agent Support function are used, mails and SNMP TRAP to report that "The DP volume capacity of the DP pool exceeded the Over Provisioning Ratio Forewarning threshold value." are issued. <Web Message> I6GK00 Over Provisioning Ratio Forewarning(Pool-x) x: pool number <Equipment model / Firmware version> DF800S/M/H, V7.0/A (0870/A) and later DF800ES/EM/EH, V9.0/A (0890/A) and later [Conditions of Occurrence] The problem occurs when all of the following conditions are met. (1) Dynamic Provisioning is enabled. (2) A DP pool is used. (3) The difference in value between Warning Alert threshold and the Limit Alert threshold of Over Provisioning Threshold for the DP pool of (2) is less than 5%. (Default: Limit Alert threshold is 130%, Warning Alert threshold is 100%.) [Cause] Firmware bug When the occurrence conditions are met, the following expression is true. Capacity that is minus 5% of Limit Alert threshold < DP pool capacity< capacity of Warning Alert threshold Due to a bug that only "whether the DP pool capacity exceeds the capacity that is minus 5% of Limit Alert threshold" is checked, the firmware notifies users of the warning even though the DP pool capacity does not exceed the Warning Alert threshold. However, the notification of inadequate warning to users does not result in limitation on DP operations. <Countermeasure> The firmware is modified to check whether the DP pool capacity exceeds the Warning Alert threshold when the DP pool capacity exceeds the Limit Alert threshold, and notify users of warning if the DP pool capacity exceeds the Warning Alert threshold. [Recovery] Apply the fixed firmware. <Action in the case of the failure> Change the Limit Alert threshold or Warning Alert threshold so that the difference between the thresholds is 5% or greater. <Web Message>	